



# Chemical Facility Anti-Terrorism Standards (CFATS)

**Integrating CFATS SSP Requirements  
and Corporate Enterprise Risk  
Management Needs**

**May 6, 2009**



## Introduction – Tim Hanley



- Vice Chairman and U.S. Process & Industrial Products Leader, Deloitte & Touche LLP
- 29+ years of experience specializing in organizational strategy and development execution, acquisitions, and market development
- Formal speaker at many industry organization events
- Frequently published in business and sector trade publications including the *Wall Street Journal*, *Reuters*, *Chicago Tribune*, *Crane's*, *U.S. Industry Today*, *Dow Jones News Wire*

# Today's speakers



**Colonel Bob Stephan**

Dutko Worldwide

Former Assistant Secretary of Homeland Security  
for Infrastructure Protection

---



**David Moore**

President & CEO

AcuTech Consulting Group

---



**Brian Geffert**

Principal

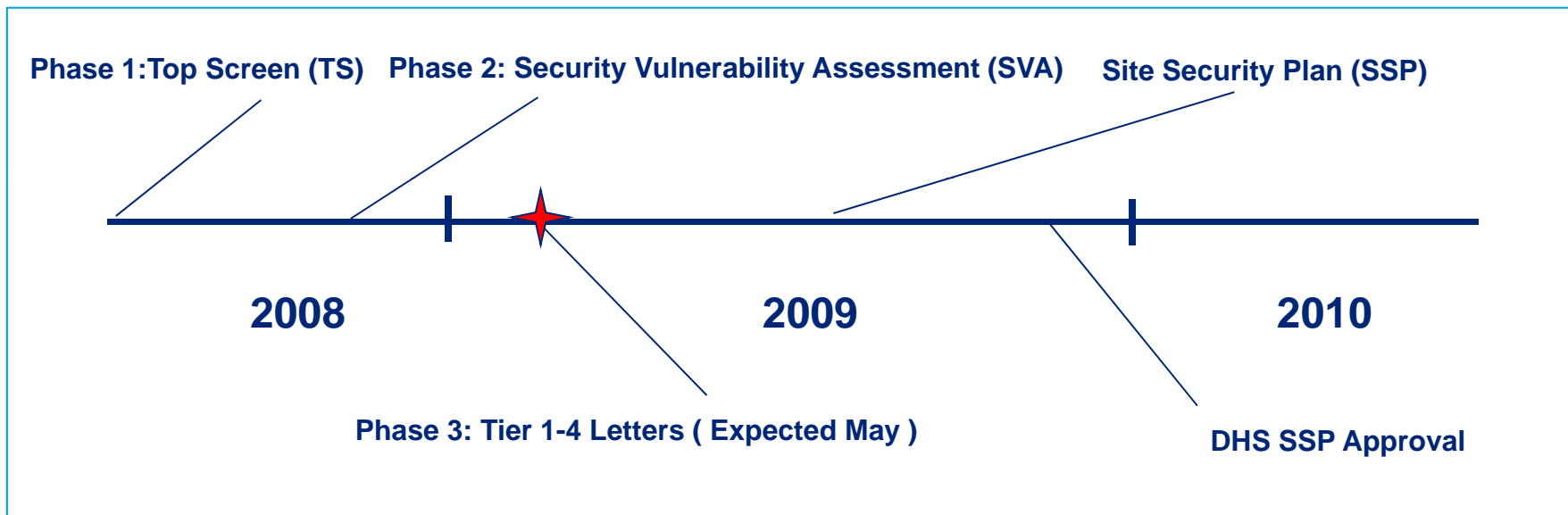
Deloitte Security &  
Privacy Services

## Session objectives

- Corporate Responsibilities: What's ahead in the Chemical Facility Anti-terrorism Standards (CFATS) process
- Developing the CFATS Site Security Plan (SSP): An Enterprise Perspective
- Understanding the long term management of SSP implementation and related CFATS requirements

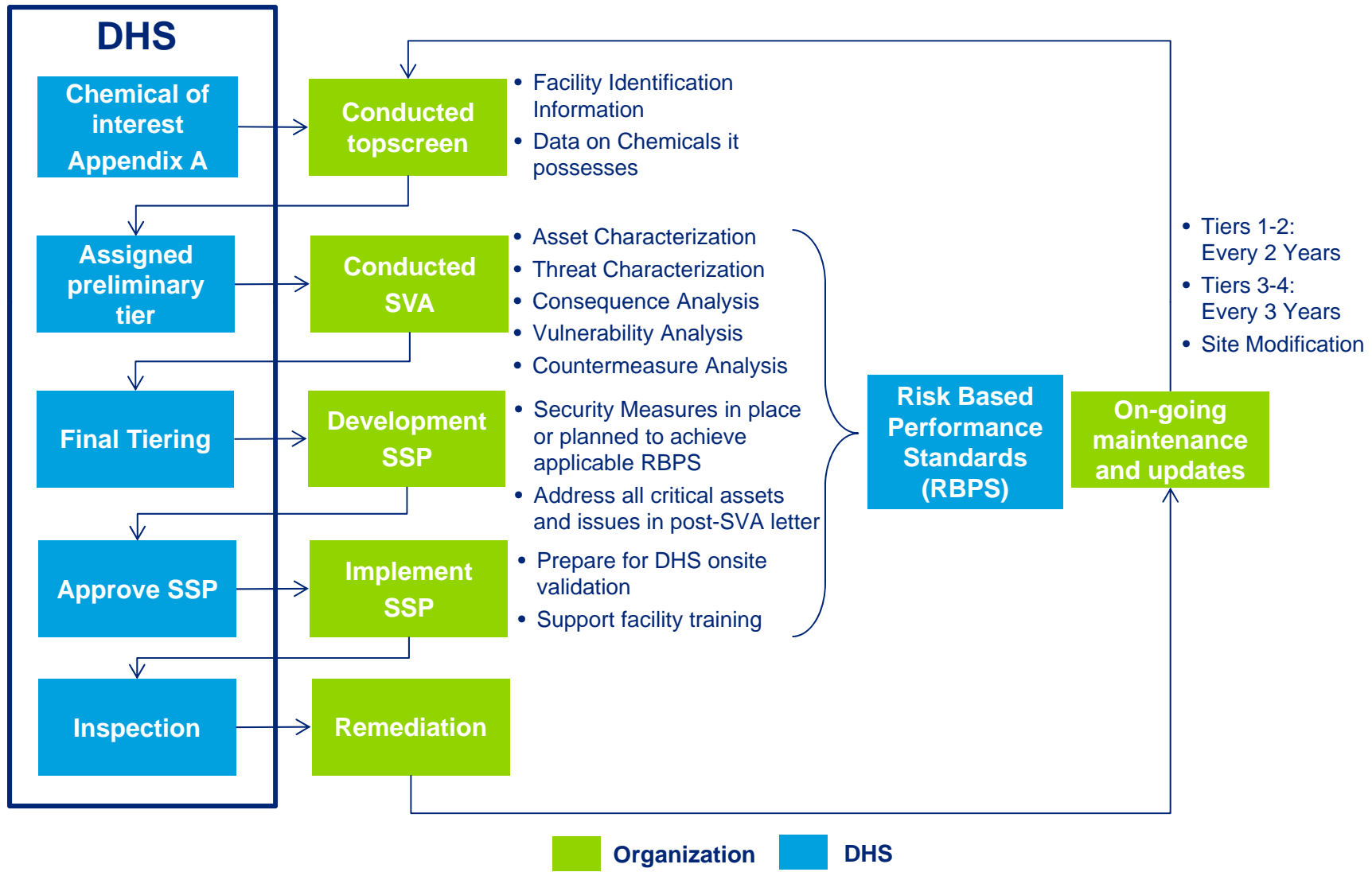
# Anticipated “Near-Term” CFATS timeline

In 2006, U.S. Department of Homeland Security (DHS) was given authority by Congress to regulate the security of “High Risk” Chemical Facilities.

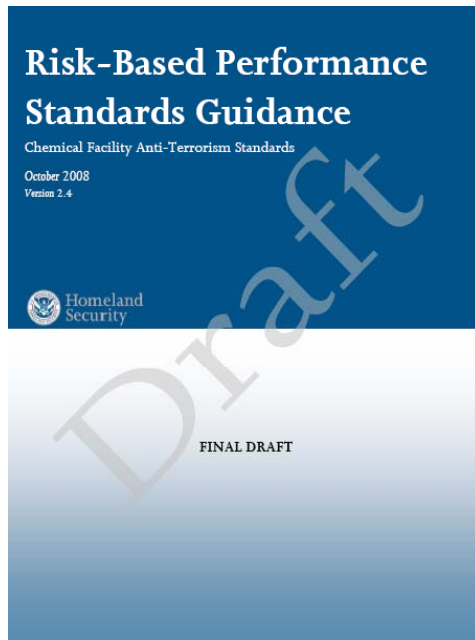


Currently, DHS has been reviewing the SVAs and will issue their final tier determinations via Letters which will be issued in a staggered sequence (30-day intervals per tier), beginning with Tier 1 facilities. Upon receipt, facilities have 120 days to submit a SSP to DHS for approval, with verification inspections to follow the SSP approval on a schedule under development by DHS.

# CFATS regulatory lifecycle



# DHS RBPS



1. Restricted Area Perimeter
2. Securing Site Assets
3. Screening & Access Controls
4. Deter, Detect, and Delay
5. Shipping, Receipt & 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 & Suspicious Activities
17. Officials & Organizations
18. Records
19. Others as determined by DHS

- RBPS guidance is not mandatory or the “preferred solution”. The guidance represents a menu of control options from which a facility may choose to mitigate facility-specific risk against a variety of threats.

# Polling question #1

**How far along in the process of building the SSP is your organization?**

- Have not started
- Have started to collect information
- Waiting for DHS Letter
- Planning to use an Alternative Security Plan (ASP)
- Finished!
- Do not know

# SSP overview

A key objective of SSP process: Reduce significant facility-level risk in a comprehensive, measurable approach, which encompass a full spectrum of physical security, cybersecurity and personnel surety requirements



- **SSPs typically outlines the following information**

- All critical assets & security issue
- Site and system boundaries
- Roles / responsibilities of all authorized individuals who manage /use the site and applicable systems
- Threats , vulnerabilities and risks associated with the site and system boundaries
- Security requirements, the current controls in place or planned controls to address risks
- On-going SSP management and maintenance requirements

- **Common inputs for developing the SSP**

- Chemical of Interest on Site
- Completed Site Vulnerability Assessment
- Site Threat Profile
- Applicable Laws & regulations
- DHS RBPS & Internal Security Requirements
- Corporate and Site Policies and Procedures

Span the continuum of “Deter, Detect, Delay, Mitigate and Respond”

# SSP scope — Systems

## Systems that:

- Control/monitor a process with a Chemical of Interest (COI) with release flammable or toxic;
- Control/monitor a process that has theft or sabotage COI
- Contains business information that if compromised may lead to one or more of the above actions
- Control/monitor a process with potential economic or governmental mission criticality (future)

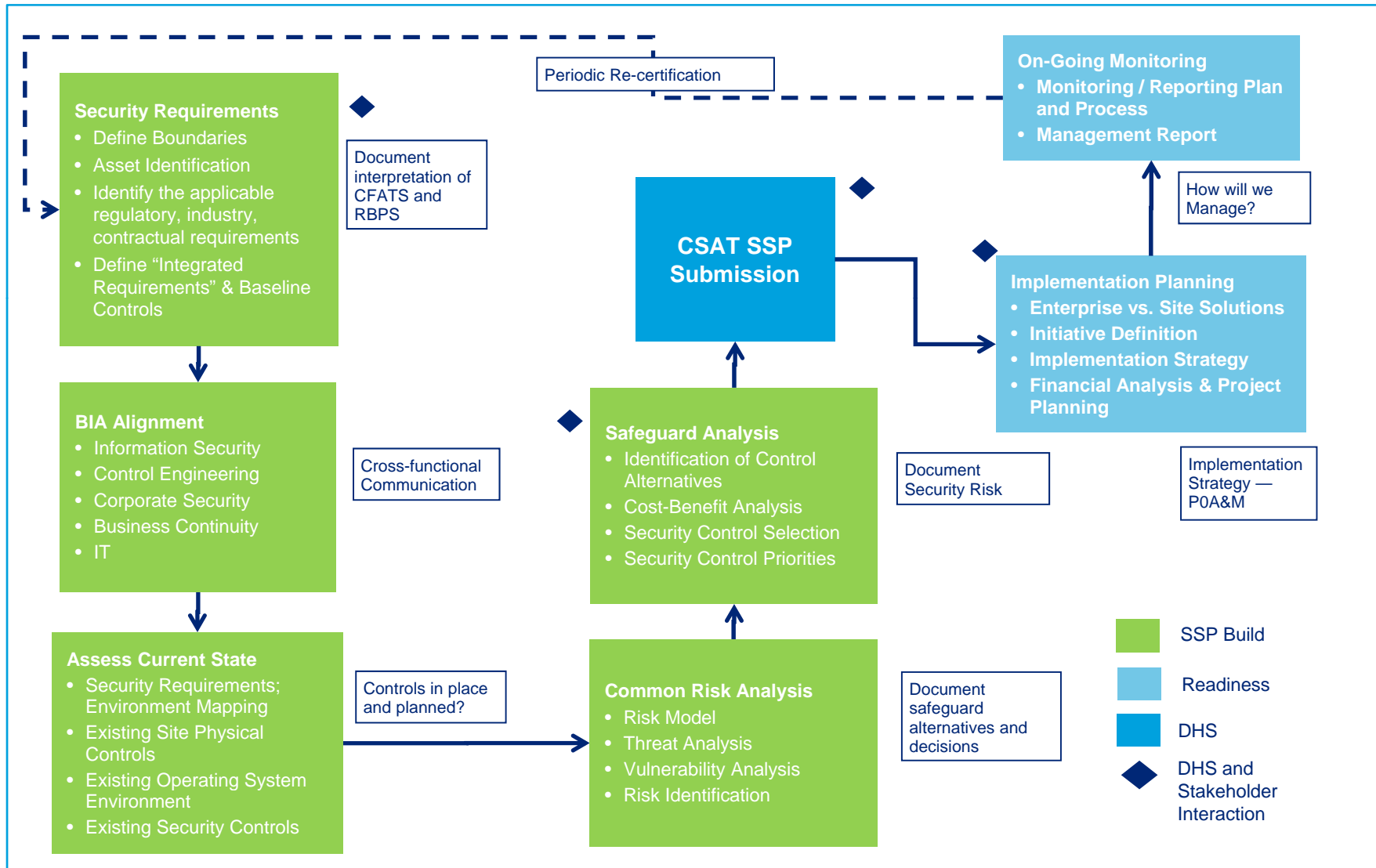
## Examples include:

- Industrial control systems (ICS) including:
  - Supervisory control and data acquisition (SCADA) systems
  - Distributed control systems (DCS)
  - Programmable logic controllers (PLC)
- Business computer systems containing relevant data
  - Inventory
  - Supply Chain
  - Personnel information
- Access control or surveillance systems particularly with internet connectivity

## Located at:

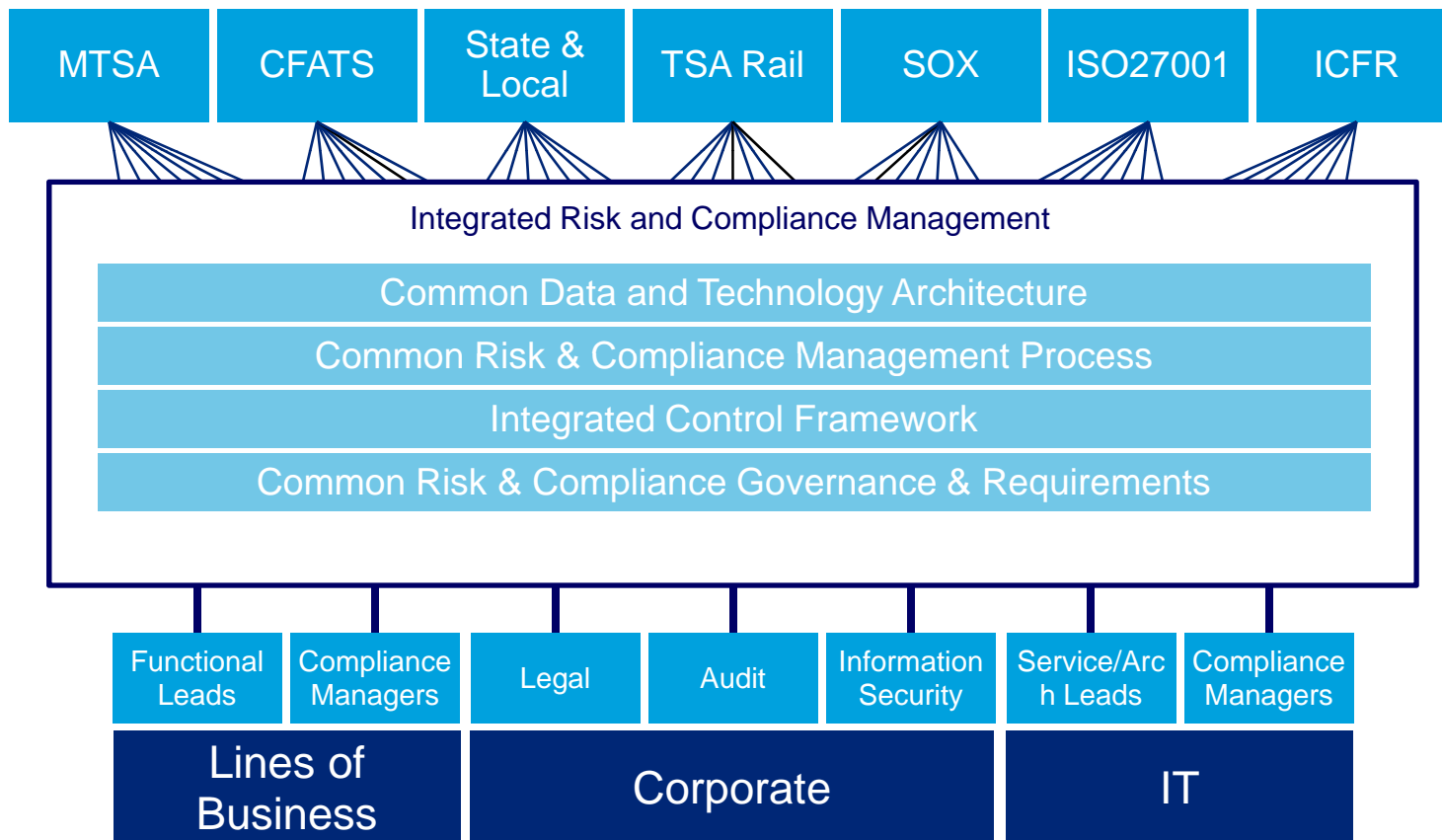
- At the regulated facility site
- Outside the geographic boundaries of its location
  - Corporate headquarters
  - Vendor's location

# SSP build approach



# The opportunity

Integrated risk and compliance management provides the opportunity to simplify the complexity created by management silos



## Polling question #2

**What unit within your organization has been assigned the lead in developing the SSP?**

- Information Security
- Corporate Security
- Regulatory Compliance
- Risk Management
- Combination of the above groups
- None of Above

## Key points to consider

The following points should be considered as you develop your organization's SSP

- Although the SSP are site-specific, consider enterprise solutions to address requirements such as training
- RBPS represent guidance only and are not meant to be prescriptive in nature — No model plan that can just be applied to your site
- SSPs will be submitted on-line tool so creation of the data for SSP will not provide a working “security plan”
- Implementing the SSPs will typically involve a combination of short-term security enhancements and long-term capital investments that can be phased in over time subject to DHS approval
- SSP development will involve dynamic interaction between your organization, DHS HQ and field inspection teams, local law enforcement and other first responders. Interaction will be key to securing final DHS plan approval
- Regulated entities may submit “Alternative Security Plans” for DHS consideration to leverage existing security protocols, capabilities and resource investments

# Enterprise considerations

SSP development should not be regarded as a “one-time” event or stand-alone exercise. The SSP can set the foundation for integrating, harmonizing and managing controls and processes across the organization at the corporate or enterprise level:

- Consistent legal assessment
- Project planning/compliance measurement
- Integration/harmonization with other regulatory programs & requirements
- Enterprise risk management
- Knowledge management/information control and protection
- Emerging threat and incident management
- Technology solutions identification/acquisition
- Cost/financial management
- Communications, governance and reporting

## Specific examples of enterprise solutions

- Corporate “CFATS Dashboard” to support long-term SSP management and on-going maintenance
- Security technology solution acquisition strategy
- Work force security awareness, education and training programs
- Security/preparedness exercise programs
- Incident response policies and protocols, and local law enforcement/first responder planning templates
- Standardized compliance documents and protected information program
- Corporate level compliance inspection templates and schedules
- Facilitated Federal grants applications to cover State/local authority responsibilities and required capabilities as defined in the SSP

## Next steps

- Conduct enterprise level review of CFATS process and SSP requirements
- Determine opportunities for enterprise vs. site-specific solutions: efficiency, cost-effectiveness, reporting, etc.
- Determine if the opportunity exists for an “Alternative Security Plan” submission and/or leveraging of previous enhancements/investments
- Develop SSP using RBPS guidance while leveraging existing plans and investments
- Identify long term CFATS program management and maintenance approach: compliance monitoring, audits, metrics, reporting, training, document control, etc.
- Determine opportunities to harmonize solutions and ongoing management of CFATS requirements with other regulatory regimes
- Conduct workshops to educate individuals on the types of controls and solutions required to address requirements, and appropriate evidence to demonstrate control working effectively — “Inspection Readiness”

Questions

# Contact information



**Tim Hanley**

Vice Chairman and U.S. Process & Industrial Products Leader  
Partner, Deloitte & Touche LLP  
thanley@deloitte.com

---



**Colonel Bob Stephan**

Dutko Worldwide  
Former Assistant Secretary of Homeland Security for Infrastructure Protection  
Bob.stephan@dutkoworldwide.com

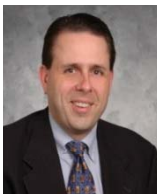
---



**David Moore**

President & CEO  
AcuTech Consulting Group  
dmoore@acutech-consulting.com

---



**Brian Geffert**

Security & Privacy Services  
Principal, Deloitte & Touche LLP  
bgeffert@deloitte.com

This presentation contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this presentation, rendering business, financial, investment, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

## About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP and Deloitte Consulting LLP, which are subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

# Deloitte.