



After the Top-Screen: Compliance with the Chemical Facility Anti- Terrorism Standards (CFATS)

***Chicago Chapter of the Academy of Certified Hazardous
Materials Managers***

February 21, 2008

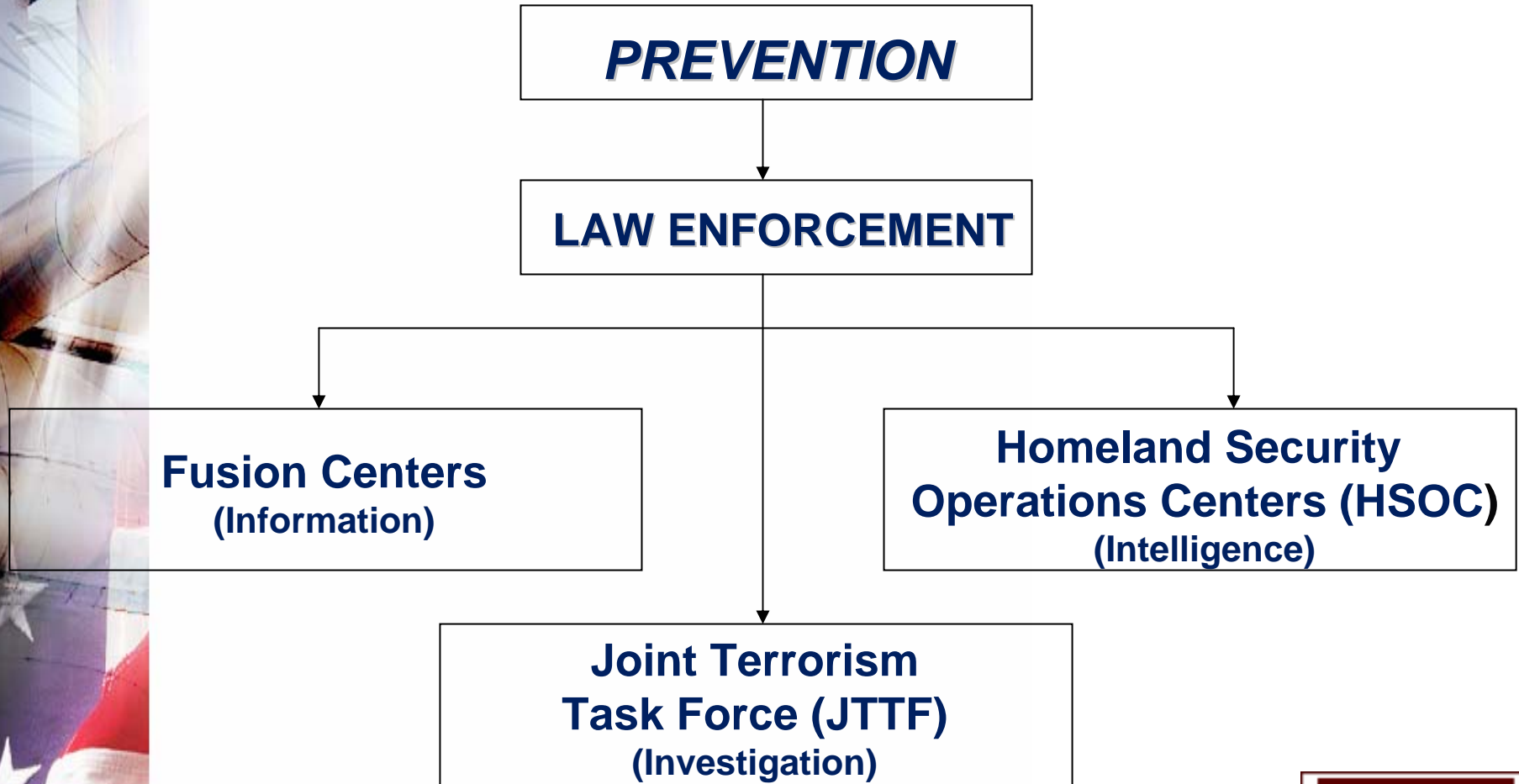
***Jeffrey P. Hullinger, P.E.
Weaver Boos Consultants***



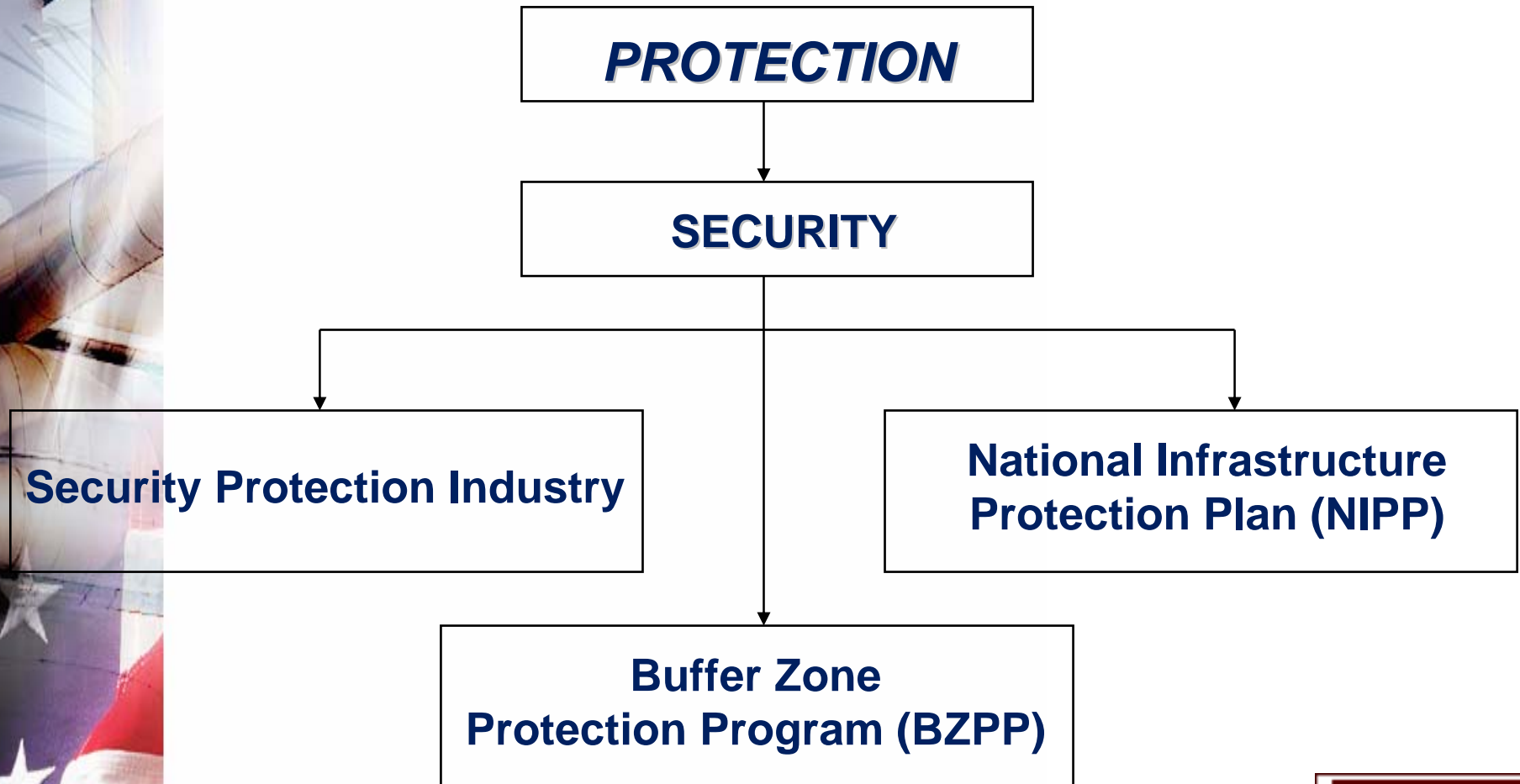
The 4 Pillars of Homeland Security

- ***PREVENTION***
- ***PROTECTION***
- ***RESPONSE***
- ***RECOVERY***

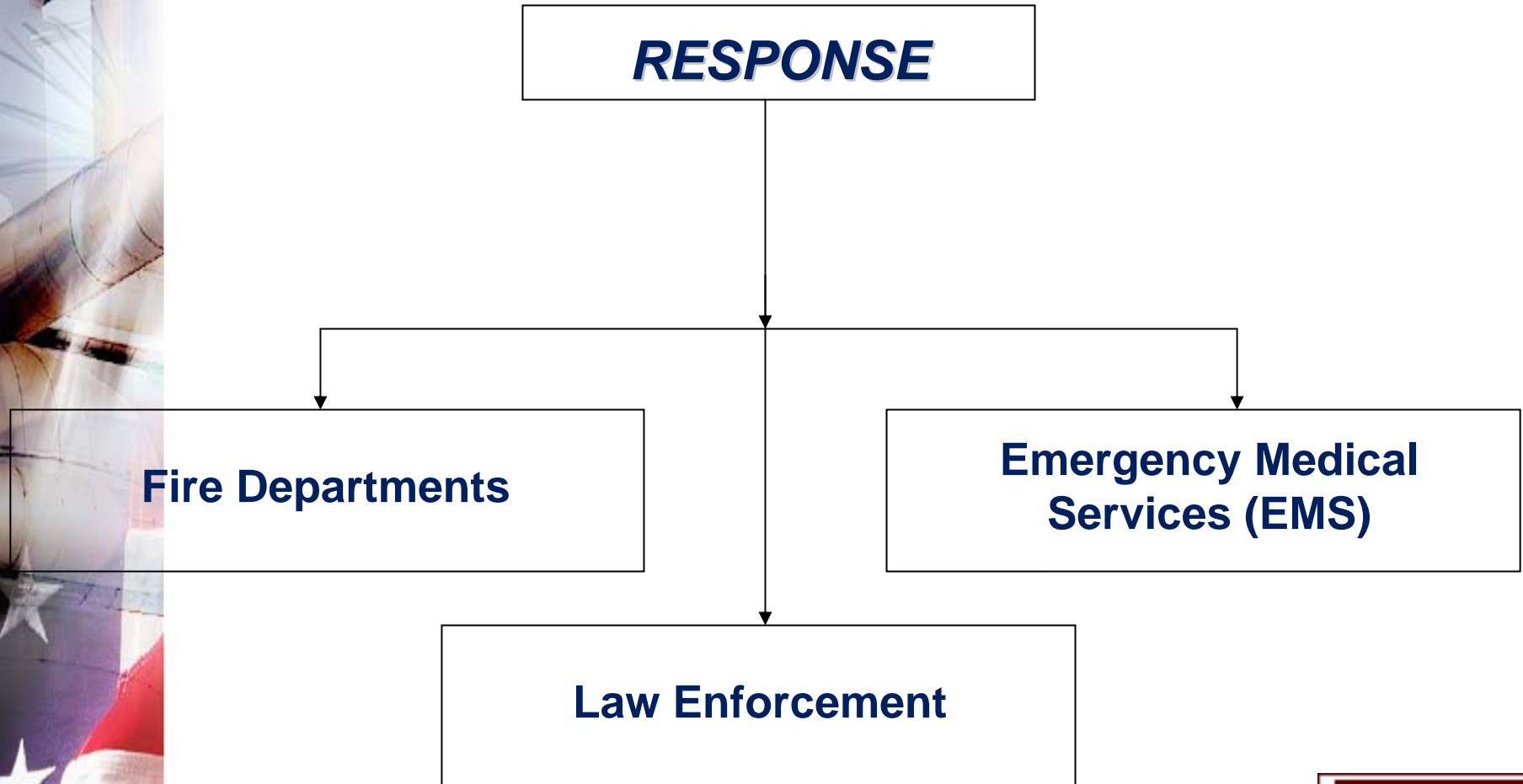
Navigating the U.S. DHS



Navigating the U.S. DHS



Navigating the U.S. DHS



Navigating the U.S. DHS

RECOVERY

**EMERGENCY
MANAGEMENT
AGENCIES (EMA's)**

County EMA
(4 hour hold)

State EMA
(72 hour hold)

Federal EMA (FEMA)
(2 year hold)



Chemical Facility Anti-Terrorism Standards

- *Directive legislation October 2006*
- *Draft Rules – published April 9, 2007*
- *Final Rules – published November 20, 2007*
- *Regulation aimed at Prevention, Protection, and Response*



6 CFR 27: Chemical Facility Anti-Terrorism Standards

- *Much lobbying, especially by propane gas suppliers (4,300 comments received; of these, 4,000 were by the propane industry)*
- *Issues with certain chemicals with threshold quantities set at “any amount”*
- *New list of chemicals developed to respond to concerns of the regulated community*



Purpose of the Regulation

- *Enhance the nation's security by lowering the risk to terrorist action posed by certain chemical facilities*
- *Provide for planning and program development to address potential threats posed by terrorist actions against chemical facilities*
- *Provide consistent requirements to “chemical facilities” (includes much more than the Chemical Process Industry)*

6 CFR 27: A Risk-Based Program

- *DHS has developed a risk-based tiering structure*
- *DHS will assign risk levels from Tier 1 (highest) to Tier 4; all these apply to “high-risk” facilities*
- *Assignment of risk tier will be based on the Chemical Security Assessment Tool (CSAT):*
 - *Top-Screen*
 - *Security Vulnerability Assessment (SVA)*

Exempted Facilities

- *Facilities covered by the Maritime Transportation Security Act (MTSA) – 33 CFR Subpart H*
 - *Primarily facilities that receive or ship via barge*
 - *See 33 CFR §105.105 for applicability*
- *Public Water Systems as defined by Section 1401 of the SDWA*
- *Treatment Works as defined in Section 212 of the FWPCA (but note – portions of facility not regulated under §212 are subject to this rule)*
- *Any Department of Defense or Department of Energy facility*
- *Any nuclear facility (regulated by the NRC)*

Regulated Facilities

- *In general:*
 - *Secretary of DHS has discretion to decide who is covered*
 - *“Any (facility) that possesses **or plans to possess**, at any relevant point in time, a quantity of a chemical ... determined ... to be potentially dangerous or that meets other risk-related criteria identified by (DHS)”*
- *Practically speaking, facilities possessing chemicals listed in Appendix A of the regulation at above screening threshold quantities (STQs)*

Regulated Facilities Census

- *Estimated total facilities covered is ~50,000, nationwide*
- *Estimated total “high risk” facilities is 5,000 to 8,000, nationwide*

Battery Limits

- *Materials in transit are not covered – but coverage of tankers and other vehicular containers begins the moment they enter a facility*
- *Facility fenceline becomes the dividing line for jurisdiction between Transportation Security Administration (TSA) and the Office of Infrastructure Protection*

Fundamentals of Security Risk

- *Risk is a function of factors:*
 - *The consequences of a successful attack (C)*
 - *The likelihood that an attack will be successful, or vulnerability (V)*
 - *Attractiveness of the target (A)*
 - *Intent and capability of an adversary, or threat (T)*
- $R = f (C, V, A, T)$



What Risks are Targeted?

- *Human Life*
- *Public Health*
- *Economic Consequences*



Threat Vectors Identified by DHS

- *Off-site release*
 - *Toxic by inhalation*
 - *Flammables*
 - *Explosives*
- *Theft or diversion – weaponization (e.g. chlorine gas used as weapon in Iraq)*
- *Theft and sabotage by contamination*



Fundamentals of Countermeasures

- **Deter**: *prevent or discourage the breach of security by instilling fear or doubt*
- **Detect**: *identification of an adversary before and/or during the attempt to commit a malicious act*
- **Delay**: *providing barriers to slow progress of adversary in penetrating a target, and/or leaving a target area to help apprehend and prevent theft*
- **Defeat**: *forces necessary to defeat adversary*



Top-Screen: Now Complete

- *What Comes Next?*
 - *Nothing, for low-risk facilities*
 - *Security Vulnerability Assessment (SVA), for others as directed by DHS*
 - *Site-Specific Security Plan, after review of the SVA, if directed by DHS*



Security Vulnerability Assessment (SVA)

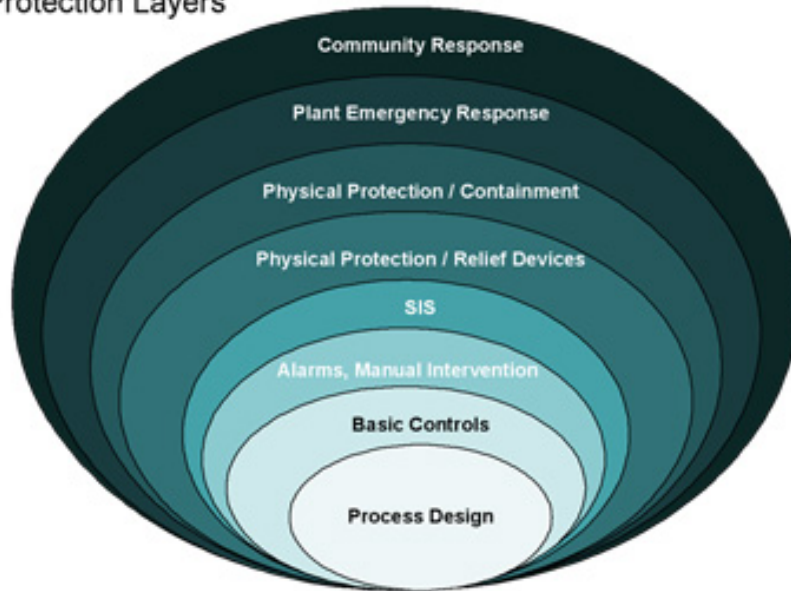
- *Phase I – Planning and Preliminary Information Collection*
- *Phase II – Facility Characterization and Threat Identification*
- *Phase III – Vulnerability Gap Analysis*
- *Phase IV – Countermeasures Identification*
- *Phase V – Reporting, Followup, and Verification*

SVA Methodology

- *Several have been tentatively approved by DHS:*
 - *Center for Chemical Process Safety (CCPS)*
 - *American Petroleum Institute (API) – based on CCPS but more specific protocols*
 - *Sandia National Laboratory – RAM-CF*
 - *Proprietary in-house models: ExxonMobil, PPG, BASF, Air Products, typically CCPS-based*
- *API model may be most broadly useful*
- *All CCPS-based models rely on Layers of Protection Analysis*

What is LOPA?

Protection Layers



Layers of protection analysis (LOPA) is a semi-quantitative methodology that can be used to identify safeguards that meet the independent protection layer (IPL) criteria.

LOPA Process

- ***Record all reference documentation***
- ***Document the security scenario under consideration***
- ***Identify all of the initiating causes for the process deviation and determine the frequency of each initiating cause***
- ***Determine the consequence of the security scenario***
- ***List the independent protective layers (IPLs) that can completely mitigate all listed initiating causes***
- ***Provide specific, implementable recommendations***

LOPA Process

- ***The result of the LOPA is a risk measure for the scenario – an estimate of the likelihood AND consequence***
- ***This estimate can be considered a “mitigated consequence frequency” – the frequency is mitigated by the independent layers of protection***
 - ***If additional risk reduction is needed, more IPLs must be added to the design***

LOPA Advantages

- ***Focuses on severe consequences***
- ***Considers all the identified initiating causes,***
- ***Encourages system perspective***
- ***Confirms which IPLs are effective for which initiating causes***
- ***Allocates risk reduction resources efficiently***
- ***Provides clarity in the reasoning process,***
- ***Documents everything that was considered,***
- ***Improves consistency of security process assignment***
- ***Offers a rational basis for managing IPLs in an operating plant***



DHS Risk-Based Performance Standards

“Covered facilities must satisfy the performance standards identified in this section. The Assistant Secretary will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable **layering of measures** used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:”

DHS Risk-Based Performance Standards

- **Restrict Area Perimeter.** Secure and monitor the perimeter of the facility
- **Secure Site Assets.** Secure and monitor restricted areas or potentially critical targets within the facility
- **Screen and Control Access.** Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including:
 - Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility
 - Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures

DHS Risk-Based Performance Standards

• ***Deter, Detect, and Delay.*** Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

- *Deter vehicles from penetrating the facility perimeter, 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 countersurveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades*
- *Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning*



DHS Risk-Based Performance Standards

- **Shipping, Receipt, and Storage.** Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility
- **Theft and Diversion.** Deter theft or diversion of potentially dangerous chemicals
- **Sabotage.** Deter insider sabotage
- **Cyber.** Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data, Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems

DHS Risk-Based Performance Standards

- **Response.** *Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders*
- **Monitoring.** *Maintain effective monitoring, communications and warning systems, including,*
 - *Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained*
 - *Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department*
 - *Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions*
- **Training.** *Ensure proper security training, exercises, and drills of facility personnel*

DHS Risk-Based Performance Standards

• **Personnel Surety.** Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

- Measures designed to verify and validate identity
- Measures designed to check criminal history
- Measures designed to verify and validate legal authorization to work
- Measures designed to identify people with terrorist ties



• **Elevated Threats.** Escalate the level of protective measures for periods of elevated threat

• **Specific Threats, Vulnerabilities, or Risks.** Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue



DHS Risk-Based Performance Standards

- **Reporting of Significant Security Incidents.** Report significant security incidents to the Department and local law enforcement officials;
- **Significant Security Incidents and Suspicious Activities.** Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
- **Officials and Organization.** Establish official(s) and an organization responsible for security and for compliance with these standards;
- **Records.** Maintain appropriate records; and
- **Address any additional performance standards the Assistant Secretary may specify.**



Contact Information

Jeff Hullinger, P.E.

Weaver Boos Consultants

jhullinger@weaverboos.com

614-487-1066

Col. Ken Morckel (ret.)

Director: Homeland Security and Law Enforcement Services

First Response Solutions, Inc.

kmorckel@firstresponsesolutions.com

614-314-8203

