



The New Federal Chemical Facility Security Regulations

Ted Cromwell
June 27, 2007





Backdrop

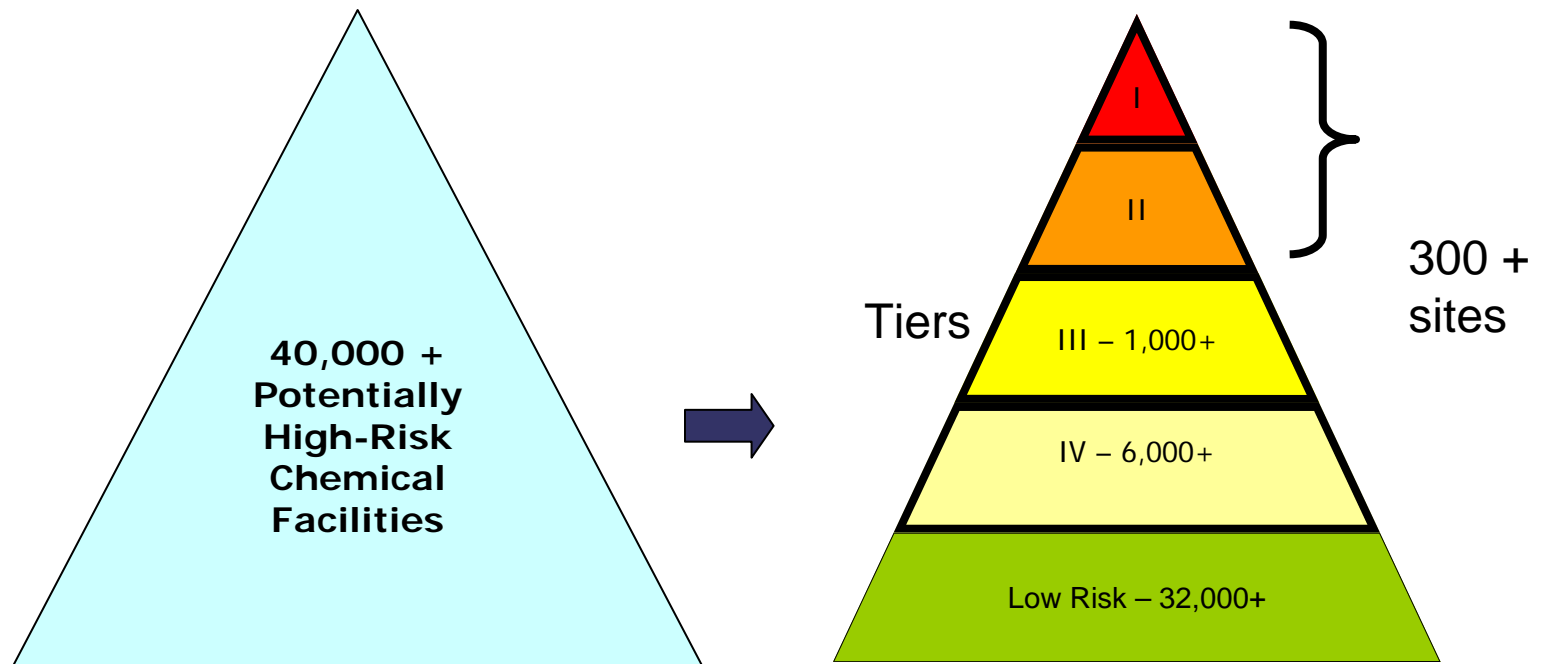
- Section 550 of FY07 DHS appropriations bill (PL 109-295, 6 U.S.C. § 121 note)
- Enacted after stalemate on S. 2145, H.R. 5695
- Signed by the President October 4, 2006
- DHS Advance Notice of Rulemaking, 71 Fed. Reg. 78276 (Dec. 28, 2006)
- Interim Final Rule, 72 Fed. Reg. 17688 (April 9, 2007)



Scope of Program

- “Chemical facilities” presenting “high levels of security risk”
- Any facility possessing > “screening threshold quantity” of ~ 360 “Appendix A” chemicals = “presumptively high risk,” must do “Top Screen” (est. 40-50,000)
- DHS then notifies covered facilities (est. 5,000), provisionally assigns to 1 of 4 risk-based tiers

DHS Chemical Facility Anti-Terrorism Standards - CFATS





Scope of Program

- Basis for coverage: harm to life or health from:
 - Toxic or flammable release (RMP)
 - Theft/diversion (CWC mainly)
 - Contamination
- In future: criticality to national security/economy
- List of chemicals, thresholds could grow over time



Scope of Program

- Exemptions for:
 - Maritime Transportation Security Act (MTSA) facilities (security regulated by Coast Guard)
 - Public drinking water systems (security regulated by EPA)
 - Sewage treatment plants (security unregulated) (but not industrial WWTPs)
 - DOE & DOD-owned or operated facilities
 - NRC-regulated facilities (NRC regulates security) (but not exempt based on small radioactive sources)



Scope of Program

- No limitations based on nature of facility, NAICS code, etc.
- Transportation-related facilities (railyards, trucking terminals) exempted for now, pending TSA action
- Multiple owner/operator facilities handled case-by-case. Will DHS honor/enforce agreements between facilities?



Basic Requirements

- Do Security Vulnerability Assessment (SVA)
- Develop & implement Site Security Plan (SSP)
- SSP to contain security measures that:
 - “Address” vulnerabilities identified in SVA
 - Meet 19 risk-based performance standards (more stringent for lower tier #s)
- Repeat every 2 years (tiers 1 & 2), every 3 years (tiers 3 & 4); after material modifications



Timing

- Rule became effective June 8
- Once Appendix A final, 60 days to do Top Screen
- DHS to respond in 60 days
- If deemed high risk, 90 days to do SVA
- DHS to respond in 60 days
- 120 days to do SSP
- Voluntarily accelerated “Phase/Track 1” for 50 or so top facilities – by Labor Day?



CSAT

- Chemical Security Assessment Tool
- Secure, Web-based application for:
 - Registration
 - Top-Screen
 - SVA
 - SSP
- DHS encourages facilities to register NOW
- Identify submitter(s), provider(s), authorizer(s)



SVA

- Tiers 1-3 must use CSAT SVA methodology
- Tier 4 can use other credible SVAMs, under concept of “alternative security program” (ASP)
- CSAT SVAM modified from “RAMCAP”
- Identify, characterize assets
- Apply standardized “terrorist attack modes” (not “design basis threats”).



SSP

- Also part of CSAT
- Any facility can propose ASP
- Address vulnerabilities
- Describe specific security measures for each performance standard



Performance Standards

- 19 categories of security performance standards; e.g.,
 - Secure, monitor perimeter
 - Control access
 - Develop, exercise emergency response plan
 - Background checks, credentialing
- Guidance due by late summer 2007 will spell out level of performance required
 - will be crucial document



Performance Standards

- Greatest concern = #4 (“Deter, Detect, Delay”). Includes requirement to:
 - “Delay an attack for a sufficient period of time so as to allow appropriate response” – requires armed guards?
 - DHS to direct \$ to local law enforcement near top-tier facilities



Performance Standards

- #12: Background checks for facility personnel, contractors & visitors w/ unescorted access to restricted area/critical assets
 - Criminal background (you do w/ commercial databases, you decide what's disqualifying)
 - Immigration status (you do)
 - Terrorist Screening Data Base (DHS does)
- Credentialing system unspecified



Inherently Safer Technology?

- DHS cannot mandate IST --
 - Standard for site security plans: DHS must “permit each . . . facility to select layered security measures that, in combination, appropriately address the vulnerability assessment and . . . performance standards for the facility”
 - Secretary may not disapprove a plan based on the presence or absence of a particular security measure. May disapprove if does not meet applicable performance standard.
 - DHS says can’t indirectly require IST via performance standards



Information Protection

- New concept: “Chemical-Terrorism Vulnerability Information” -- like USCG/TSA “sensitive security information” (SSI)
- CVI may be shared with state/local officials “possessing the necessary security clearances”; they may not disclose it under state/local law
- In enforcement actions, CVI to be treated as if classified
- No access to CVI for other civil litigation, says DHS
- Criteria for “high risk”/not, tier dividing lines *classified*



Enforcement

- DHS must review & approve each vulnerability assessment and site security plan, inspect facilities
- 30 officers from Federal Protective Services detailed as inspectors; finishing training now
- If DHS finds violation, must give facility:
 - Clear, written explanation of deficiencies
 - Opportunity for consultation
 - Order to comply by a date that DHS determines is “appropriate under the circumstances”



Enforcement, con't

- If facility does not comply with order, DHS may:
 - Impose civil administrative penalty of up to \$25,000 per violation (same as MTSA)
 - “Issue an order for the facility to cease operation, until the owner or operator complies with the order.”
- Adjudication rules, with appeal process to Under Secretary. Then off to court.
- But what's reviewable? Much discretion for DHS.



Preemption

- Section 550 is silent on preemption
- DHS says conflict preemption applies automatically:
 - State law preempted if actually conflicts with or frustrates purpose of federal program
 - E.g., if state law limited a facility's flexibility to choose security measures?
 - Same as Coast Guard position re facility security
- Can seek DHS opinion on preemption



Preemption

- Only state/local security programs now: NJ, NY, MD, Baltimore
- ACC does not believe any of these programs, as currently implemented, are preempted by the federal program.
- Preemption not self-implementing; someone would have to file a lawsuit and persuade a federal judge.



Sunset?

- “[T]he authority provided by this section shall terminate three years after the date of enactment of this Act.”
- DHS says it could consider a future appropriations law continuing funding for the program post sunset date to be an extension of the “authority provided by this section.” Comptroller General Opinions support this view.



Continued Legislation Assured

- Iraq War supplemental appropriations bill did not include any language that would have amended Section 550:
- FY08 DHS appropriations (House version) does address S. 550 – focused on preemption
- Eventual authorizing bills



Thank You

Ted Cromwell, Sr. Director Security and
Operations

Ted_Cromwell@americanchemistry.com

