



Security Vulnerability Assessment (SVA)

- Follows the SVA approach established by CCPS and others
 - Asset Characterization: assets associated with chemicals identified in the post Top-Screen letter
 - Threat Characterization: specific scenarios prescribed by CSAT
 - Risk Analysis: potential consequence of scenarios against identified assets and the likelihood of success of an attack
 - Vulnerability Analysis: security measures in place to mitigate or reduce the likelihood of success of an attack on an asset
 - Countermeasures Analysis: strategies that reduce the probability of a successful attack or the degree of success

Cont'd



Security Vulnerability Assessment (SVA) (cont)

- Both physical and procedural controls are considered in the elements of an SVA:
 - Physical site vulnerability
 - Fencing, Lighting, Camera
 - Security Guards, Alarms
 - Restricted Access Areas
 - Personnel vulnerability
 - Cyber vulnerability



Submission Requirements

- Tiers 1,2, and 3 must submit an SVA using the online CSAT tool
- Tier 4 facilities may submit Alternate Security Program (ASPs) for consideration in lieu of the online CSAT tool
 - ASP must include vulnerability analysis
 - ASP must meet all requirements of the rule for SVA and provide for an equivalent level of security



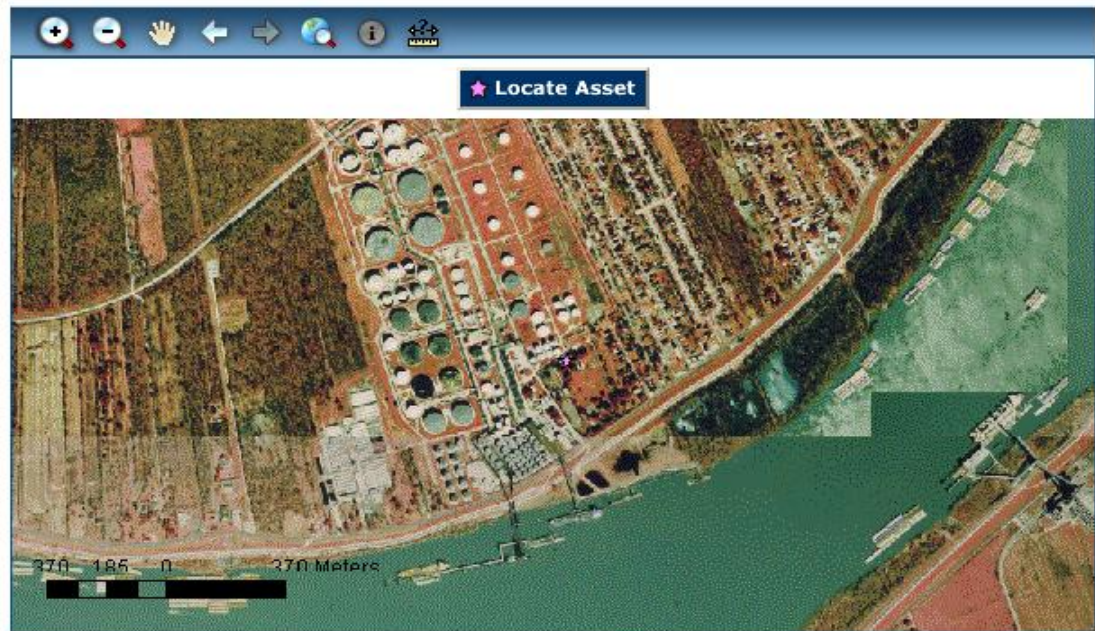
Critical Asset

- SVA must identify each “Critical Asset” for regulated chemical of concern
- SVA process assesses each Critical Asset individually
- Definition of “Critical Asset”
 - ??????????????
- Should be defined in SVA guidance document being developed by DHS



Locating Critical Assets

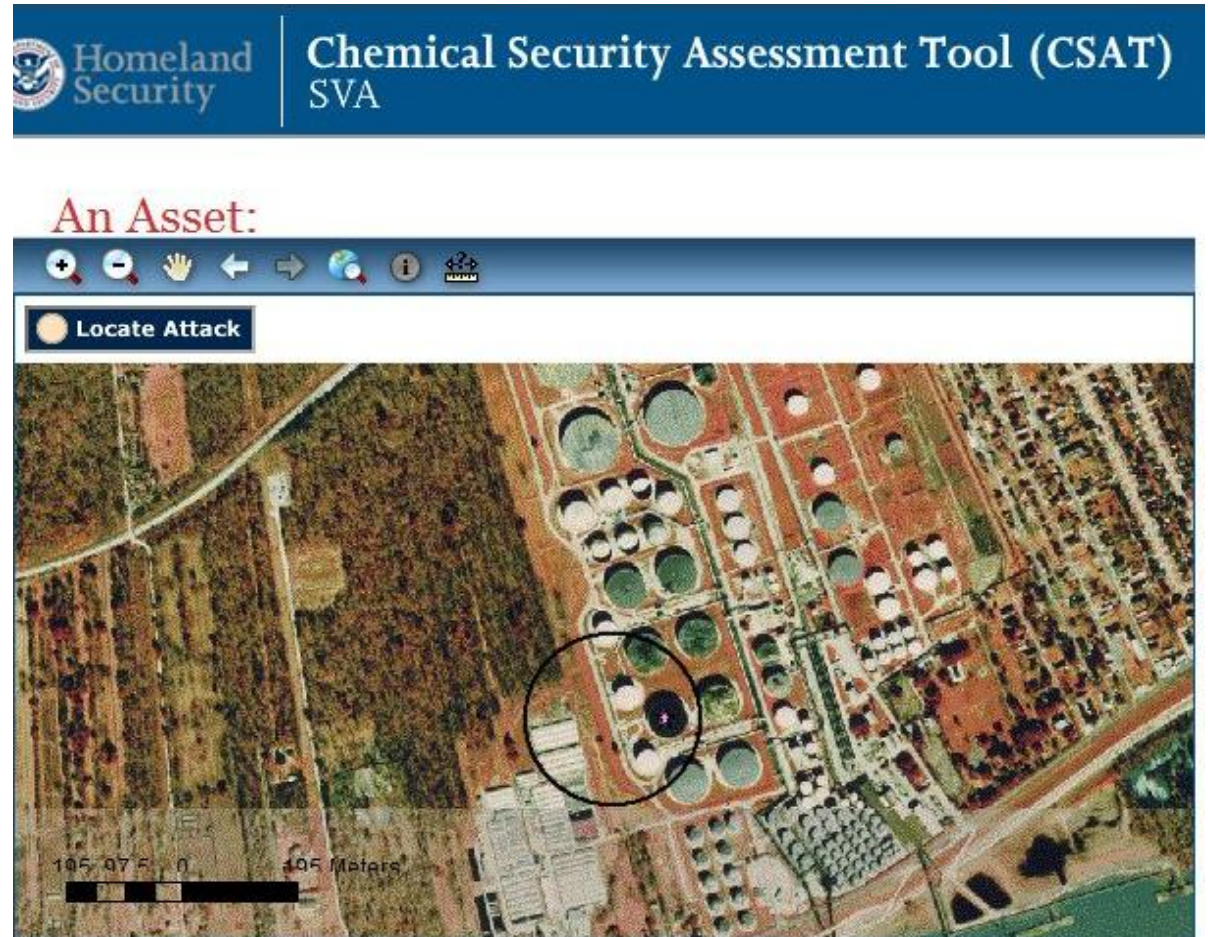
- CSAT provides up to 1m resolution
- Enables a facility to upload image if necessary





Identify Attack Location

- Each critical asset is identified
- The location of attack is identified
- Judgment of preparer and submitter as to impacts
- Reasonableness verified during DHS inspection





SVA Output

- Informs facility of tier of each critical asset based on potential consequences
 - Tier Level information may be available as each asset SVA is completed
- Final facility tier is based on highest asset-specific tier

Cont'd



SVA Output Cont'd

- Generates a CVI protected letter to each facility that includes:
 - Final facility tier
 - Asset specific tier ranking and the associated security issue
 - Defines the next steps required by the facility
- Information in post-SVA letter used by facility during CSAT SSP to identify the applicable RBPS based on asset tiers and security issues