



Texas Chemical Sector — Small & Mid-Size Facility Pain Points

A partnership briefing for Critical Infrastructure Outreach

Prepared by the IHS Chemical Sector Project Manager: Jeff Hernandez

Purpose

This briefing maps the operational, regulatory, and security pressures facing small and mid-size chemical facilities in Texas. It is designed to do two jobs at once: orient the IHS Chemical Sector program to the realities its future partners live with, and supply credible, current talking points for first-contact outreach. Leading with a facility's problems rather than a generic partnership ask is what earns the meeting.

Why Small & Mid-size Facilities Are Different

The mega-majors run mature, well-funded security and compliance organizations. The small and mid-size producers, blenders, and distributors that make up the long tail of the Texas chemical sector generally do not. They carry many of the same hazards and obligations but with thin margins, few or no dedicated security or compliance staff, and limited capacity to track a fast-moving regulatory landscape. That gap between exposure and capacity is precisely where a university-based, non-regulatory partner like IHS can add value — as a trusted advisor rather than an enforcer.

The Pain Points

1. Security Gap after the CFATS lapse

Congress allowed the statutory authority for the Chemical Facility Anti-Terrorism Standards (CFATS) program to expire on July 28, 2023, and it remains lapsed. CISA can no longer inspect high-risk sites, require physical or cyber security measures, or run terrorist-database vetting of personnel with access to dangerous chemicals (*Cybersecurity and Infrastructure Security Agency [CISA], n.d.*). For roughly 3,200 previously high-risk facilities, the federal security baseline and the free tools that came with it simply went away, even though the underlying risk did not. CISA now points facilities to its voluntary ChemLock program, but voluntary uptake among resource-constrained facilities is uneven.



INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY®

Where IHS can help: The lapse is the single clearest opening for outreach. IHS can offer the assessment and planning support facilities lost, framed around the ChemLock voluntary model essentially filling the gap without the “compliance stick”.

2. Process Safety Compliance in flux (EPA RMP)

EPA's 2024 Risk Management Program Safer Communities by Chemical Accident Prevention (SCCAP) took effect in May 2024, with most prevention program requirements due by May 10, 2027. It expands the program in ways that hit smaller operators hard: mandatory natural-hazard and power-loss evaluation in process hazard analyses, safer-technology alternatives analysis, root-cause incident investigation, and third-party audits. The rule traces directly to the 2013 West, Texas fertilizer explosion. Complicating matters, EPA announced in March 2025 that it was reconsidering SCCAP and, in February 2026, proposed a “Common Sense Approach” rollback, with the comment period extended into May 2026 (*U.S. Environmental Protection Agency [EPA], 2024, 2026; U.S. Small Business Administration [SBA] Office of Advocacy, 2026*). Facilities are left preparing for 2027 deadlines against a moving target.

Where IHS can help: IHS can help facilities cut through the uncertainty by interpreting current SCCAP obligations, supporting the new natural-hazard and power-loss analysis, and running readiness reviews so they are neither caught short nor over-investing in requirements that may change.

3. Cyber and OT/ICS exposure

Industrial control environments are an accelerating target. Analysts reported roughly a 40% rise in internet exposed ICS devices between 2024 and 2025, and in February 2026 CISA flagged a December 2025 operational technology attack that hit more than 30 energy and combined-heat-and-power facilities, using wiper malware against remote terminal units and human-machine interfaces with direct implications for chemical operators running similar edge devices (*CISA, n.d.; Dragos, 2026*). The recurring themes are industrial ransomware aimed at disrupting supervision and control, poor IT/OT network segmentation, and third-party vendor remote access as an entry vector. Smaller facilities rarely have OT-specific security coverage.

Where IHS can help: IHS cybersecurity can deliver Operational Technology / Industrial Control System (OT/ICS) assessments, Information Technology/ Operational Technology (IT/OT) segmentation reviews, and vendor access and incident response planning scaled to facilities without a dedicated security team.



INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY®

4. Physical Security & Insider Threat

With CFATS enforcement gone, perimeter security, access control, and protection against theft or diversion of chemicals of interest fall entirely to the facility. Small sites often lack layered physical security, formal visitor and contractor controls, or insider-threat awareness of the very areas CFATS site security plans used to structure.

Where IHS can help: IHS security assessments can evaluate perimeter, access control, and diversion risk; drone-based surveys can extend that to large or hard-to-access sites efficiently.

5. Natural Hazard & Weather Resilience

Texas facilities sit in the path of recurring, high-consequence natural hazards. Gulf hurricanes, inland flooding, and the kind of hard freeze seen in Winter Storm Uri (2021), which knocked out power and triggered process upsets and releases across the state. Loss of power and utilities is a leading pathway to accidental release, which is exactly why the updated RMP rule now folds natural hazards and power loss into hazard analysis. Smaller operators frequently lack robust continuity-of-operations and backup-power planning.

Where IHS can help: IHS can support continuity-of-operations and hardening reviews and use aerial assessment for pre-storm vulnerability surveys and rapid post-event damage evaluation.

6. Supply Chain & Logistics Fragility

The sector's dense concentration along the Gulf Coast corridor is efficient yet vulnerability. Feedstock dependence, single-source suppliers, and reliance on rail, pipeline, and port throughput mean a disruption at one node cascades. Movement of toxic-inhalation-hazard materials by rail and truck adds a transportation-security dimension that smaller shippers are not always equipped to manage.

Where IHS can help: IHS can help partners map critical dependencies and single points of failure and connect transportation-security concerns to the division's broader corridor and supply-chain work.

7. Emergency Preparedness & Community Coordination

Effective response depends on relationships built before an incident — with Local Emergency Planning Committees, mutual-aid partners, and first responders who may

not know a small facility's hazards or layout. Tier II reporting and exercises are often treated as paperwork rather than readiness, and drills are infrequent at smaller sites.

Where IHS can help: IHS can design and facilitate exercises, review emergency response plans, and help facilities strengthen LEPC and first-responder relationships.

Pain Point → IHS Capability Map

A one-look summary for tailoring the conversation to what a given facility is worried about:

Pain point	How IHS can help	IHS service line
Security Gap after CFATS lapse	Voluntary security vulnerability assessments; site security plan review; help adopting CISA ChemLock-style practices.	Security Assessment
Process-safety / RMP in flux	Help interpreting SCCAP obligations & 2027 deadlines; natural-hazard & power-loss PHA support; readiness reviews.	Security Assessment
OT/ICS Cyber Exposure	OT/ICS cyber assessments; IT/OT segmentation review; vendor remote-access & incident-response planning.	Cybersecurity
Physical Security & Insider Threat	Perimeter, access-control & chemical-of-interest theft/diversion assessments.	Security Assessment / Drone
Natural Hazard & Weather Resilience	Continuity-of-operations planning; aerial pre/post-storm assessment; hardening reviews.	Drone / Security Assessment
Port / Waterway-adjacent Facilities	Maritime security & MTSA compliance support for Ship Channel and coastal sites.	Maritime Compliance
Emergency Preparedness & Coordination	Exercise design; LEPC / first-responder relationship building; plan reviews.	Security Assessment



INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY®

Sources

- **Cybersecurity and Infrastructure Security Agency.** (n.d.). *Chemical Facility Anti-Terrorism Standards (CFATS)*. U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats>
- **Dragos.** (2026, February 17). *Dragos 2026 OT/ICS cybersecurity report and year in review*. <https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware>
- **U.S. Environmental Protection Agency.** (2024, February 27). *Risk management program: Safer communities by chemical accident prevention final rule*. <https://www.epa.gov/rmp/risk-management-program-safer-communities-chemical-accident-prevention-final-rule>
- **U.S. Environmental Protection Agency.** (2026, February 24). Common sense approach to chemical accident prevention. *Federal Register*, 91(36), 11200–11225. <https://www.epa.gov/rmp/common-sense-approach-chemical-accident-prevention-proposed-rule>
- **U.S. Small Business Administration, Office of Advocacy.** (2026, April 6). *EPA extends comment period for proposed Risk Management Program updates*. <https://advocacy.sba.gov/2026/04/06/epa-extends-comment-period-for-proposed-risk-management-program-updates/>