Vol. 17
Editor: Shelby Payne

August 2026

The Resilience Rundown

The Security Gap Texas Chemical Facilities Can't Afford to Ignore

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

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.

Cyber and OT/ICS exposure

Industrial control environments are an accelerating target — internet-exposed ICS devices rose roughly 40% between 2024 and 2025, and in February 2026 CISA flagged a December 2025 attack that hit 30+ energy and power facilities using wiper malware against control systems, with clear implications for chemical operators running similar equipment. Common themes: industrial ransomware, weak IT/OT segmentation, and third-party remote access as an entry point. Smaller facilities rarely have dedicated OT security.

Read the Whole Article Here

RESEARCH

Online Research Link

Unseen Threats to Texas Critical Infrastructure: The Risk to Buried Utilities and Targeted Policy Solutions to Protect Them

Benjamin Dierker

Excavation damage to underground infrastructure is a costly but preventable problem that hits Texas hardest, yet proven technology, practices, and policy reforms can nearly eliminate it.

Excavation damage to underground infrastructure is a nationwide problem, ranging from minor disruptions to lethal, regional crises, that is almost entirely preventable. Texas is uniquely at risk due to its concentrated energy infrastructure, growing population, and constant development, and routinely leads the nation in damage incidents, costing billions in economic harm each year. Proven solutions, including validated technology, best practices, and policy reform, can reduce this damage to virtually zero, sparing lives, saving dollars, and protecting critical infrastructure.

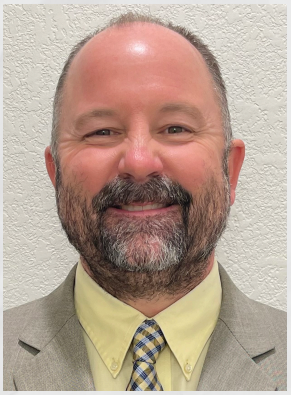
IHS is proud to announce the national publication of Holding Back Disaster, published by Routledge and grown directly out of IHS research into excavation damage — a preventable, costly problem that hits Texas harder than almost anywhere in the country.

The book pairs peer-reviewed research rigor with real-world storytelling and live QR code resources, making it as engaging as it is authoritative. It's built to work as a classroom text, an industry training and onboarding tool, a leadership briefing resource, and a reference for policymakers alike.

Holding Back Disaster is available now through Routledge.

STAFF HIGHLIGHT <<<

Erik Peterson
Project Manager



Erik Peterson is a Project Manager at Sam Houston State University's Institute of Homeland Security, where he leads the Critical Manufacturing Sector. A federal agent and peace officer for over 33 years, he served 17 years as an NCIS Special Agent (2020 Agent of the Year) and three years as a US Army CID Cyber Agent, with 15 years embedded with FBI Task Forces on counterintelligence and cyber intrusion investigations. He later rose to Lieutenant with the Texas Department of Public Safety, supervising Critical Infrastructure Engagement within the Homeland Security Division. Peterson holds a B.S. in Criminal Justice from Sam Houston State University.

Read More of his background on the IHS Website

>>> EVENTS <<<

Disruptions in Healthcare: Identifying and Mitigating

August 20, 2026

Livestream

More information: here

AI at the Crossroads: Impacts at the Nexus of Critical Infrastructure

August 28, 2026

Livestream

More information: here

PODCAST <<<

Calculating Criminal & Structural Social Networks
with Dr. Nathan Jones & Braell Dotson

Every actor is within six degrees of separation from Kevin Bacon. We can measure and chart that professional network - and we can do it with Mexican drug cartels and critical infrastructure assets. This week, we chat with Dr. Nathan Jones, professor and chair of the Security Studies department at Sam, and Braell Dotson, an enterprising recent graduate who coded a plugin to open-source software used by law enforcement to measure and track criminal networks.

Listen to the Podcast: HERE