Vol. 14
Editor: Shelby Payne

March 2026
Designer: Emily Hayde

IHS NEWSLETTER

Energy Sector Security Emerging Trends

Critical infrastructure security has been moving toward integrated, intelligence-driven, and resilience-focused models. Organizations that align cybersecurity with operational continuity and invest in partnerships, and workforce development will be best positioned to handle evolving threats. As the energy sector becomes more digital and decentralizes, cybersecurity risk becomes inseparable from grid reliability. Private industry that integrates operational technology (OT) security, strengthen supply chains, and prioritize resilience will be better equipped to withstand evolving threats as they occur.

Attackers are developing malware and techniques tailored to energy infrastructure, targeting SCADA systems and safety controls at power generation facilities or substations. This marks a shift from IT disruption to potential physical consequences. Energy providers face growing ransomware risk not just to data but to uptime. Threat actors are targeting operational continuity, knowing power outages create immediate pressure to pay or meet their demands.

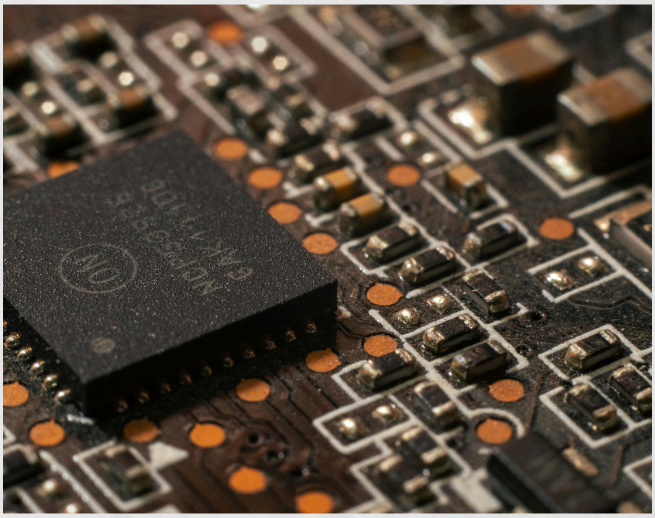
RESEARCH

Online Research Link

Regulating Artificial Intelligence in the State of Texas: Challenges and Opportunities

Alexander Kinney, Ph.D

Developing a comprehensive regulatory approach for artificial intelligence remains a challenging prospect.



In recent years, several states have moved to implement such frameworks. With the passage of the Texas Responsible Artificial Intelligence Governance Act (TRAIGA) in June of 2025, Texas established itself as a leader in this effort. The act aims to balance the need to promote innovation through artificial intelligence with the need to mitigate risk. Unsurprisingly, the intentions of this policy have deep implications for critical infrastructure resilience. The aim of this technical paper is to evaluate the potential impacts of this new policy on AI governance, review its potential impact on businesses operating in critical infrastructure sectors, and highlight opportunities for strengthening this foundational piece of legislation. In what follows, I will provide a brief overview of the significance of regulating AI development and misuse, review the risks associated with AI misuse, and describe complementary state level efforts to regulate AI that have been enrolled into law. I will then provide an overview of TRAIGA and suggest several ways that future legislative efforts can improve on the provisions outlined in this act.

TEAM MEMBER HIGHLIGHT

Robert Crane

Program Manager

Robert Crane is a homeland security professional specializing in critical infrastructure resilience. Since 2022, he has served as Program Manager at the Institute for Homeland Security at Sam Houston State University, focusing on infrastructure security and resilience. He retired from federal service in 2020 after serving as the U.S. GPS and Positioning, Navigation, and Timing (PNT) Resilience Advisor at the Department of Homeland Security, where he helped align national policy across space, cybersecurity, and infrastructure resilience efforts and advised the Space-Based PNT Executive Committee. Mr. Crane's career also includes leadership roles within DHS and more than 26 years of service in the U.S. Coast Guard, supporting maritime security and national contingency operations.

EVENTS

TRANSPORTATION CRITICAL INFRASTRUCTURE SYMPOSIUM

MAY 5TH, 2026

This event moves beyond awareness and theory to prioritize practical, actionable mitigation strategies delivered by industry practitioners—not long lectures or sales pitches. Sessions will be structured around moderated panels, encouraging real-world discussion and lessons learned.

MARITIME RISK SYMPOSIUM

JUNE 2-3RD, 2026

Over 90% of global trade travels through the world's maritime domain, making it a linchpin of international commerce. Safeguarding this vast ecosystem is vital—not only for the secure transport of goods and passengers, but also for economic resilience and national security.

PODCAST

INTERNET INFRASTRUCTURE AND DISCONNECTING DISSENT

DR. KARPOOR SHASHIDHAR AND DR. CIHAN VAROL

This week, we chat with Dr. Karpoor Shashidhar and Dr. Cihan Varol of the computer science department at Sam Houston State about internet infrastructure at home and abroad. We also talk with Scott McHugh, program executive for the private sector at the Institute for Homeland Security, about the geopolitics of internet disconnection and access.

Link: https://ihsonline.org/ihs-media/podcast

$settings_function = null, $settings_file = null) {
$settings_function, $settings_file);
object. Base attribute is required', 'js
$attributes);