ALERT

Texas Cyber Command: New Authority for Statewide Cybersecurity Coordination

Texas enacted HB 150 to create the Texas Cyber Command, centralizing cybersecurity for public entities and influencing vendor and contractor obligations.

By Austin Chegini, Aimee P. Ghosh, Brian E. Finch

TAKEAWAYS

- HB 150 established a centralized cybersecurity body under the University of Texas System for state and local agencies.
- Private contractors may face new cybersecurity terms in state procurement and contracts.
- Critical infrastructure firms can opt in for support, triggering reporting and coordination duties.

07.17.25

On June 2, 2025, Texas Governor Greg Abbott signed House Bill 150 into law, establishing the Texas Cyber Command, a component institution of the University of Texas System focused on strengthening cybersecurity across Texas government. Rather than adding a new regulator, the law establishes a centralized authority to coordinate cyber operations, threat response and readiness across public-sector entities.

While the Command's authority applies only to governmental bodies, its creation signals a shift in how the state organizes its cybersecurity posture. This new law may have practical implications for vendors, contractors and other private-sector partners that interact with state and local agencies.

What HB 150 Does

The law establishes the Texas Cyber Command as a component institution of the University of Texas System, administratively attached to the University of Texas at San Antonio. The Command consolidates

cybersecurity functions previously managed by the Department of Information Resources (DIR), serving as the state's centralized authority for public-sector cybersecurity operations.

Its core mission is to coordinate cyber readiness, threat intelligence and incident response across the state's public institutions, including state agencies, local governments and institutions of higher education. The law tasks the Command with a range of operational, advisory and support responsibilities, including:

- **Incident Response and Recovery.** The Command is responsible for leading coordinated responses to cybersecurity incidents that impact public entities. It also provides digital forensics support, post-incident analysis and technical assistance to help agencies recover and mitigate further risk.
- **Threat Monitoring and Intelligence.** A core function of the Command is to operate a 24/7 threat intelligence center and cybersecurity hotline. This capability allows it to gather, analyze and share threat indicators with state and local agencies in real time.
- **Policy and Standards for Public Entities.** The Command is tasked with developing statewide cybersecurity standards and best practices for use by government agencies. It also oversees mandatory training programs to ensure that public employees are equipped to identify and respond to cyber risks.
- **Operational and Strategic Support.** Beyond incident response, the Command will assist public entities with vulnerability assessments, remediation planning and strategic risk management. It is also charged with supporting regional coordination efforts and building the state's long-term cybersecurity workforce.

While the Command holds rulemaking authority for public-sector cybersecurity policy, it is not a regulator in the conventional sense. It cannot impose penalties, mandate private-sector compliance or dictate technology choices to companies operating outside the scope of government contracts.

That said, as the Command's standards become embedded in procurement and operational frameworks, private vendors and contractors may face new compliance expectations when doing business with the state, especially in areas like IT services, cloud computing and infrastructure support.

Who Does HB 150 Affect?

The Texas Cyber Command's formal authority under the law is limited to public-sector entities, but its influence will extend beyond that scope, particularly through procurement, coordination and contracting practices.

State and Local Government Agencies

These agencies are the Command's primary focus and are expected to comply with new statewide cybersecurity protocols.

They will be responsible for:

- implementing minimum cybersecurity standards,
- reporting cyber incidents to the Command within required timeframes,
- ensuring employee completion of state-approved cybersecurity training, and

- participating in coordinated incident response efforts.

The law marks a shift from decentralized IT management toward a more unified model for cyber operations.

Institutions of Higher Education

Public colleges and universities fall within the Command's scope, with policy implementation developed in consultation with existing higher education governance structures.
Institutions should plan to:

- align internal practices with statewide cybersecurity standards,
- meet mandatory training and reporting obligations, as defined in collaboration with the state, and
- coordinate with the Command during cyber events or investigations.

While some flexibility exists through consultative processes, alignment is expected to tighten over time as standards mature.

Private Sector Vendors and Contractors

While private companies are not directly subject to the Texas Cyber Command's authority, those doing business with state or local government entities will be affected through procurement standards and contract requirements.

Vendors may be expected to:

- comply with cybersecurity standards referenced in RFPs and prequalification processes,
- agree to contract terms involving breach reporting, audit access or cybersecurity training, and
- extend these obligations to subcontractors handling government data or systems.

These requirements will be especially relevant for cloud-service providers, managed-service providers (MSPs), software vendors and systems integrators supporting public-sector clients. As the Command's standards become embedded in statewide procurement practices, vendors will likely face more uniform and enforceable cybersecurity expectations.

These expectations will ultimately depend on how individual agencies integrate Command-issued standards into their procurement policies and contracting practices.

Critical-Infrastructure Operators

Private entities operating in sectors such as energy, transportation and health care are not automatically subject to the Texas Cyber Command's authority; however, under the new law, they may become "covered entities" if they enter into contracts with the Command to receive cybersecurity services.

Once designated as covered entities, these operators may be subject to obligations including:

- reporting cybersecurity incidents to the Command,

- coordinating with the Command during cyber incidents, and
- aligning with applicable cybersecurity policies and standards.

This designation is contractual and voluntary, meaning operators are not compelled to become covered entities; however, participation may be beneficial for entities seeking enhanced cybersecurity support and collaboration with state resources.

As agencies begin to interpret and apply the provisions of Texas's law, private-sector partners should prepare for downstream changes in procurement and contract requirements.

What to Expect Going Forward

While the act does not impose direct legal obligations on private entities, it will reshape how Texas public agencies approach cybersecurity in contracts, partnerships and procurement.

Those with business or operational ties to Texas public entities should prepare for the following developments:

- **Procurement Changes.** Expect cybersecurity requirements to appear more formally in RFPs, vendor prequalification and award criteria. Even if not explicitly attributed to the Texas Cyber Command, these standards may reflect its internal guidance to agencies.
- **Tighter Contractual Expectations.** Existing and future contracts may include new provisions around breach reporting, audit access, cybersecurity training and adherence to state-developed practices. Vendors supporting IT systems, cloud platforms or critical data should revisit terms such as SLAs, indemnities and cyber-risk allocation.
- **Critical-Infrastructure Engagement.** Private-sector operators in sectors like energy, water and transportation may become "covered entities" under the law if they contract with the Cyber Command for cybersecurity services. This designation can bring reporting, coordination and operational-alignment obligations—particularly during incident response or resilience efforts.
- **Alignment with Federal Frameworks.** Clients operating under NIST, Federal Risk and Authorization Management Program (FedRAMP), or Cybersecurity Maturity Model Certification (CMMC) should monitor how Texas's approach evolves. Even when frameworks are broadly compatible, minor state-specific deviations could introduce duplicative requirements or increase complexity for vendors working across jurisdictions.

For many businesses, early awareness and proactive contract review will be essential. Aligning with emerging expectations now can reduce risk, minimize future compliance gaps and create a competitive advantage as agencies transition under the new cybersecurity structure.

Pillsbury is closely monitoring developments related to Texas Cyber Command and is ready to help clients address its evolving requirements. We advise on regulatory strategy, public-sector contracting, cybersecurity risk, incident response planning and compliance with state and federal standards. Our team

helps clients adapt procurement practices, update contract terms and manage the operational impact of Texas's new cybersecurity framework.

*(This alert is part of our **Texas Legislative Session 2025 in Review** series, designed to help readers navigate the evolving legal landscape and prepare for what lies ahead. In it, Pillsbury's multidisciplinary team of attorneys offers in-depth analysis of the most consequential developments—what passed, what stalled and what it all means for stakeholders across key industries.)*