# Texas Cyber Command

## Strategic Implementation and Operational Blueprint

August 2025

## Executive Summary

The State of Texas, through the passage of House Bill 150, has embarked on a landmark initiative to redefine statewide cybersecurity with the creation of the Texas Cyber Command (TCC). Facing a relentless barrage of cyber threats from hostile foreign actors and criminal organizations targeting the state's vast economy and critical infrastructure, the TCC's mission is to establish a centralized, proactive, and resilient defense for the state's public entities.[1] This document presents a comprehensive strategic blueprint for the TCC's structure, implementation, and long-term operation. It is designed to guide the Command's leadership, the Governor's Office, and the Legislature in transforming legislative intent into a world-class operational reality.

The TCC is envisioned not merely as a state agency, but as the central hub of a "Whole-of-Ecosystem" security model. This model extends beyond traditional state and local government collaboration to deeply integrate the unparalleled federal military, intelligence, and academic cybersecurity assets located in San Antonio.[1] By leveraging its unique administrative attachment to The University of Texas at San Antonio (UTSA), the TCC is positioned to build a sustainable talent pipeline, drive innovation, and create a formidable force multiplier for the state's defense.[3]

This blueprint outlines a detailed organizational architecture, a sophisticated technology stack centered on a statewide Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform, and the formation of specialized operational units, including a Critical Incident Response Unit, deployable Field Remediation Teams, and a state-of-the-art Digital Forensics Laboratory. Furthermore, it proposes a hybrid funding model that balances a historic $135 million direct appropriation with a strategic cost-recovery mechanism for advanced services, ensuring both foundational security for all and long-term financial sustainability.[3]

A phased, multi-year implementation roadmap provides a clear, measurable path from foundational build-out to full operational capability. By executing this strategy, the Texas Cyber Command will not only secure the state's digital assets and ensure the continuity of government services but will also establish Texas as the undisputed national gold standard in state-level cybersecurity.[6]

# Part I: Foundational Framework: Mandate, Governance, and Strategic Posture

The successful implementation of the Texas Cyber Command hinges on a clear and comprehensive understanding of its legislative mandate, the adoption of a forward-looking strategic posture, and the establishment of a robust governance framework that ensures accountability, effectiveness, and public trust.

## 1.1 Analysis of House Bill 150: Defining the Operational Charter

House Bill 150, signed into law on June 2, 2025, serves as the foundational charter for the Texas Cyber Command, outlining its purpose, authority, and structure.[4] A thorough analysis of this legislation is the essential first step in developing an operational strategy that is fully aligned with legislative intent.

### Core Mandate

The primary mandate of the TCC is to serve as the state's "centralized authority for public-sector cybersecurity operations".[4] This represents a significant strategic shift, consolidating critical cybersecurity functions that were previously managed by the Department of Information Resources (DIR) into a single, purpose-built agency.[4] The TCC's mission is explicitly defined as defending against cyber threats, leading coordinated incident response, and facilitating recovery for a wide range of public and private entities.[1] The legislation tasks the Command with a broad set of responsibilities, including operating a 24/7 threat intelligence center, developing statewide security standards, overseeing mandatory training, and providing direct operational support to affected organizations.[4]

### Scope of Authority

The law delineates a clear scope of authority for the TCC. Its formal, direct authority applies to all "governmental bodies," which includes state agencies, local governments (municipalities and counties), and public institutions of higher education.[4] These entities are now required to adhere to a new set of obligations,

including implementing minimum cybersecurity standards developed by the TCC, reporting cyber incidents within specified timeframes, ensuring employees complete state-approved cybersecurity training, and actively participating in coordinated incident response efforts led by the Command.[4]

### Opt-In Model for Critical Infrastructure

For the private sector, particularly owners and operators of Texas's vast critical infrastructure—encompassing sectors such as energy, water, healthcare, and transportation—the TCC's role is one of partnership rather than regulation.[7] These private firms can voluntarily opt-in to receive support from the TCC. However, this decision carries significant implications; once a firm opts in, it becomes subject to mandatory reporting and coordination duties during a cyber incident.[4] This voluntary framework presents both an opportunity and a challenge. While it avoids imposing a regulatory burden on private industry, it also means the state's most vital infrastructure may operate outside the TCC's direct visibility until a crisis is already underway. The TCC's success in this area will depend on its ability to demonstrate overwhelming value, making partnership an indispensable component of any critical infrastructure operator's risk management strategy.

### Administrative Structure

HB 150 establishes a unique administrative structure for the TCC, designating it as a "component institution of the University of Texas System, administratively attached to the University of Texas at San Antonio".[4] This model is deliberately designed to leverage the immense cybersecurity expertise concentrated at UTSA and within the broader San Antonio ecosystem, which is home to the second-largest concentration of cyber professionals in the nation, including key federal partners like the Sixteenth Air Force (AFCYBER), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI).[1] The Command is to be led by a Chief appointed by the Governor with the advice and consent of the Senate, ensuring executive-level accountability and a direct line to the state's highest office.[5] This placement within a university system, while advantageous for talent acquisition and research, introduces a potential for administrative friction between the agile, high-tempo needs of a security operations center and the traditionally more deliberative processes of academic governance. This necessitates a clear and formal Memorandum of Understanding (MOU) between the TCC and the UT System to define operational independence,

delegated authorities for the Chief, and service-level agreements for administrative functions like HR and procurement.

### Non-Regulatory Status

The legislation is explicit in defining the TCC's role as operational, not regulatory. The Command holds rulemaking authority for public-sector cybersecurity policy but cannot impose financial penalties, mandate private-sector compliance (outside of government contracts), or dictate specific technology choices to private companies.[4] Its influence over the private sector will be exerted indirectly, primarily through new cybersecurity terms and standards embedded in state procurement and contracts.[4] This distinction is critical: the TCC's power derives from its operational capabilities, its control over information, and its role as the state's lead coordinator, not from a punitive regulatory mandate.

## 1.2 A "Whole-of-State" Vision for Texas: The Centralized Hub for Partnerships

The establishment of the TCC provides Texas with the opportunity to implement a robust "Whole-of-State" cybersecurity strategy. This modern approach recognizes that in an interconnected digital environment, a state's overall security is only as strong as its weakest link, and that isolated, siloed defenses are insufficient against coordinated adversaries.[8]

### Defining the Model

A Whole-of-State strategy fosters a cooperative framework where state, local, tribal, and territorial (SLTT) government entities collaborate to share resources, exchange threat intelligence, and standardize defensive capabilities.[8] The goal is to create a unified front that achieves economies of scale, eliminates redundant efforts, and raises the baseline of security for all participants, from large state agencies to small rural school districts.[9]

### Adapting for Texas: A "Whole-of-Ecosystem" Approach

While many states pursue a "bottom-up" or federated approach where local entities drive participation, HB 150 has endowed Texas with a "top-down," centralized model led by the TCC.[12] This structure provides a powerful advantage in driving standardization, managing costs, and enabling enterprise-level visibility and response.[11] However, the TCC's true strategic potential lies in evolving beyond a simple "Whole-of-State" model to a more comprehensive "Whole-of-Ecosystem" model. The Command's co-location with federal military and intelligence partners in San Antonio is a unique strategic asset that must be fully operationalized.[1] This means the TCC's mission is not just to coordinate among Texas SLTTs, but to serve as the formal bridge that brings the capabilities and intelligence of partners like AFCYBER and the NSA to bear on the defense of Texas's public networks and critical infrastructure. This requires establishing formal mechanisms such as joint task forces, embedded liaison officers, and secure, real-time intelligence sharing platforms to translate this proximity into a decisive operational advantage.

## 1.3 Governance, Oversight, and Civil Liberties

To be effective and maintain public trust, the TCC requires a governance structure that balances its powerful operational mandate with robust oversight and a firm commitment to privacy and civil liberties. The legislative analysis of HB 150 identified concerns regarding its broad powers and a lack of statutory protections for collected data, which must be proactively addressed.[7]

### Internal Governance

HB 150 authorizes the TCC Chief to establish ad hoc advisory committees to support the Command's mission.[5] It is recommended that the Chief immediately charter two standing advisory bodies:

- **Technical Advisory Council (TAC):** This council should consist of Chief Information Security Officers (CISOs) from major state agencies, representatives from the Texas Association of Counties and the Texas Municipal League, and technical leaders from key critical infrastructure sectors. The TAC's role would be to provide expert, practitioner-level advice on the development of statewide standards, the selection of shared technologies, and the refinement of operational procedures.

- **Academic and Workforce Council:** This council should be co-chaired by a senior leader from UTSA and include representatives from other major Texas university systems, community colleges, and private sector training organizations. Its mission would be to guide the TCC's long-term workforce development strategy, ensuring academic curricula are aligned with the state's needs and fostering a robust talent pipeline.[4]

### External Oversight and Accountability

Building and maintaining public and legislative trust is paramount. The concerns about the TCC's authority and potential for privacy overreach are legitimate and must be addressed through a framework of transparency and accountability.[7] To this end, the following actions are recommended:

- **Enhanced Legislative Oversight:** The Legislature should consider amending the TCC's governing statute to move the Sunset review date from September 1, 2031, to September 1, 2029. This would allow for an earlier, more timely evaluation of the Command's performance and structure during its critical growth phase. Furthermore, the creation of a standing Joint Legislative Oversight Committee on Cybersecurity would provide a dedicated, expert forum for continuous monitoring and policy guidance every biennium.[7]
- **Data Privacy and Civil Liberties Framework:** The TCC must, as one of its first official acts, develop and publicly publish a comprehensive Data Privacy and Civil Liberties Policy. This policy must go beyond generic statements and establish clear, binding rules on the collection, storage, use, and dissemination of any cybersecurity data obtained from public or private entities. Critically, it must mandate that any data sharing with federal agencies or third parties be subject to a formal privacy impact assessment and a transparent notification process for the affected entities, addressing the specific statutory gaps identified in the analysis of HB 150.[7]

## Part II: Organizational Architecture and Human Capital Strategy

A sound organizational structure and a forward-thinking human capital strategy are the twin pillars that will support the TCC's mission. The Command must be organized for speed, clarity, and effectiveness, while simultaneously building a sustainable pipeline of talent to win the long-term war for cybersecurity expertise.

### 2.1 Proposed Organizational Structure for the Texas Cyber Command

The organizational structure of the TCC must reflect its diverse missions, from 24/7 network monitoring to long-term policy development. The proposed structure below is hierarchical, ensuring clear lines of command and control during a crisis, while also creating distinct directorates focused on specialized functions. This model draws inspiration from the mature organizational design of entities like the Virginia Information Technologies Agency (VITA) and incorporates all functions mandated by HB 150.[5]

**Figure 1: Proposed Organizational Chart for the Texas Cyber Command**

Chief

- Chief of Staff
- General Counsel
- Deputy Chief
    - Director of Operations
        - Cyber Threat Intelligence Center (24/7 SOC)
        - Critical Incident Response Unit (CIRU)
        - Field Remediation Teams (Regional)
    - Director of Technology & Engineering
        - SIEM & SOAR Engineering
        - Network & Infrastructure Security
        - Platform Services
    - Director of Forensics & Investigations
        - Digital Forensics Lab
        - Threat Hunting & Malware Analysis
    - Director of Governance, Risk, and Compliance (GRC)
        - Policy & Standards
        - Training & Workforce
        - Risk & Vulnerability Assessment
        - Agency & Partner Liaison
    - Director of Administration & Finance
        - Budget & Finance
        - Human Resources
        - Procurement & Contracts

This structure creates five primary directors under the Deputy Chief, each with a clear and distinct mission:

- **Operations:** The front line of cyber defense, housing the 24/7 watch floor and the primary response teams.
- **Technology & Engineering:** The builders and maintainers of the TCC's advanced technology platforms.
- **Forensics & Investigations:** The deep technical analysis unit for incident response and proactive threat discovery.
- **Governance, Risk, and Compliance (GRC):** The policy, training, and partnership arm that works to raise the security baseline across the state.
- **Administration & Finance:** The business backbone of the Command.

### 2.2 Key Leadership Roles and Responsibilities

- **Chief:** As the Governor's appointee, the Chief is the ultimate authority for the TCC, responsible for setting the strategic vision, interfacing with the Legislature and the Governor's Office, and managing the highest-level partnerships with federal and private sector entities. During a major statewide cyber crisis, the Chief serves as the principal cybersecurity advisor to the Governor.[5]
- **Director of Operations:** This role is the Command's operational heart, responsible for the 24/7 readiness and execution of its defensive and response missions. The Director manages the day-to-day tempo of the Cyber Threat Intelligence Center (CTIC) and takes direct command of the CIRU and Field Remediation Teams during significant incidents.
- **Director of Governance, Risk, and Compliance (GRC):** This Director leads the TCC's critical mission to uplift the entire state's security posture. This involves developing the statewide standards, overseeing the mandatory training programs, and managing the vulnerability assessment services offered to public entities.[4] This directorate must be staffed with professionals who are "bilingual"—fluent in both the deep technical aspects of cybersecurity and the bureaucratic and political realities of state and local government. Their role is not simply to be an auditor but a consultant and partner, helping under-resourced entities achieve compliance rather than merely punishing them for failing to do so.

### 2.3 Workforce Development and Retention Strategy

The single greatest long-term challenge to the TCC's success will be attracting and

retaining elite cybersecurity talent. State governments consistently struggle to compete with private sector salaries and hiring agility, a top concern for state CIOs nationwide.[15] The TCC's initial staffing plan calls for 65 full-time employees, doubling by 2027.[2] To meet this goal and build a sustainable workforce, the TCC must adopt a multi-pronged strategy. The initial hiring wave must prioritize platform engineers to build the core SIEM and SOAR infrastructure before the full complement of security analysts is brought on board. It is inefficient to hire dozens of analysts with no effective tools to use; the "factory" must be built before all the "workers" are hired.

### Leveraging the UTSA Partnership

The TCC's administrative attachment to UTSA is its most powerful tool for workforce development and must be fully exploited.[3] The strategy should include:

- **A Formal "Cyber Corps" Pipeline:** Establish a dedicated internship and co-op program that functions as a direct pipeline from UTSA's cybersecurity degree programs into full-time roles at the TCC. This program should offer security clearances and real-world operational experience, making it a highly competitive alternative to private sector internships.
- **Curriculum and Research Integration:** The TCC should work directly with UTSA faculty to ensure that academic curricula are aligned with the operational needs of the Command and the NICE Cybersecurity Workforce Framework.[18] The TCC can also provide anonymized, real-world data to support academic research, creating a virtuous cycle of innovation.
- **Practitioner-as-Educator Program:** Following the successful model of the Louisiana State Police partnership with LSU, senior TCC technical staff should be encouraged and incentivized to serve as adjunct faculty at UTSA, bringing invaluable, up-to-the-minute operational experience into the classroom.[19]

### Modernizing Human Resources Practices

The TCC cannot succeed if it is bound by traditional, slow-moving government HR processes. It must advocate for and implement modern talent management practices:

- **Job Classification and Compensation Reform:** The TCC must work with the UT System and the Legislature to create specialized cybersecurity job classifications with flexible, market-competitive salary bands. Standard government IT job titles and pay scales are inadequate for attracting talent in this high-demand field.[15]

- **Expedited Hiring Authority:** Seek delegated authority to implement an expedited hiring process for critical cybersecurity positions, with a goal of reducing the average time-to-hire from months to under 30 days to avoid losing top candidates to more agile private sector employers.[15]
- **Skills-Based and Diverse Hiring:** Shift the focus from rigid degree requirements to demonstrated skills, industry certifications (e.g., GIAC, CompTIA, CISSP), and hands-on experience. This broadens the applicant pool to include highly skilled individuals from community colleges, military service, and other non-traditional backgrounds.[21]

## Part III: The Technological Core: A Unified Security Operations Platform

The heart of the Texas Cyber Command's operational capability will be its technology stack. A modern, integrated, and scalable security platform is essential to provide the statewide visibility and response capabilities mandated by HB 150. This platform will be centered around three core components: a Cyber Threat Intelligence Center, a statewide SIEM, and a SOAR platform for automation.

### 3.1 Architecture of the Cyber Threat Intelligence Center (CTIC)

As required by law, the TCC will establish and operate a 24/7 Cyber Threat Intelligence Center (CTIC) and a corresponding cybersecurity hotline.[4] This CTIC will serve as the state's nerve center for cybersecurity, functioning as a central hub for monitoring, analysis, and information sharing. Its primary functions will be to gather threat intelligence from a wide array of sources, analyze that intelligence for relevance to Texas entities, and disseminate timely, actionable alerts and reports to stakeholders across the state.[1]

The CTIC's effectiveness will depend on its ability to fuse intelligence from diverse sources, including:

- **Commercial and Open-Source Feeds:** Subscriptions to leading commercial threat intelligence providers and continuous monitoring of open-source channels.
- **Government and Partner Sharing:** Establishing secure, automated data exchange with federal partners like CISA and the FBI, national partners like the Multi-State ISAC (MS-ISAC), and the TCC's unique federal partners in San Antonio.[1]
- **Organic Intelligence:** The most valuable intelligence will be generated internally from the TCC's own operations—gleaned from the statewide SIEM, endpoint security tools, and data collected during incident response engagements.

### 3.2 Statewide SIEM Implementation Strategy

A Security Information and Event Management (SIEM) platform is the cornerstone of any modern Security Operations Center (SOC). It aggregates, correlates, and analyzes log data from across the enterprise to detect potential threats and malicious activity.[22] For the TCC, the SIEM is the primary tool for achieving statewide visibility.

#### Technology and Architecture

The TCC should procure a next-generation SIEM platform capable of handling the immense scale of data from across the state. The recommended architecture is a **data lake model**, which decouples the log storage from the analytics engine. This provides two key advantages: it allows for the cost-effective, long-term retention of raw log data for compliance and historical analysis, and it enables the use of more advanced analytics tools, including machine learning and AI, against the data repository.[24]

#### Data Ingestion and Use Cases

The implementation of a statewide SIEM is as much a political and policy challenge as it is a technical one. The cost of ingesting and storing petabytes of data is significant, and forcing under-resourced local governments to bear this cost could create substantial friction.[24] Therefore, a tiered data ingestion strategy is required:

- **Tier 1 (Mandatory, State-Funded):** All executive branch state agencies will be required to forward a defined set of critical security logs to the TCC SIEM. This includes high-value sources like authentication logs (Active Directory), firewall and VPN logs, cloud identity provider logs (e.g., Azure AD), and alerts from endpoint detection and response (EDR) agents.[25] The cost for this baseline visibility will be covered by the TCC's direct appropriation.
- **Tier 2 (Optional, Cost-Recovery):** Local governments, school districts, and other public entities can opt-in to have their logs monitored by the TCC. This would be offered as a fee-for-service, allowing them to leverage the state's enterprise-class SIEM at a fraction of the cost of procuring their own.[5]

The SIEM will be configured with detection rules and analytics models tailored to threats facing government entities, such as ransomware precursors, insider threats

identified through User and Entity Behavior Analytics (UEBA), and abuse of legitimate administrative tools.[22]

### 3.3 SOAR Integration for Automated Defense

The sheer volume of alerts generated by a statewide SIEM would quickly overwhelm a human-only analysis team. A Security Orchestration, Automation, and Response (SOAR) platform is the necessary force multiplier. SOAR platforms integrate with the broader security toolset (SIEM, EDR, firewalls) to automate the repetitive, time-consuming tasks associated with incident triage and response, freeing up human analysts to focus on complex threats.

The TCC's SOAR implementation will focus on developing a library of automated "playbooks" to handle common security events. Initial playbooks should target high-volume, low-complexity alerts where a high degree of confidence allows for automated action:

- **Phishing Email Triage:** Automatically extract URLs and attachments from user-reported phishing emails, analyze them in a sandbox environment, and if malicious, automatically block the associated indicators across the state's networks and email gateways.
- **Endpoint Containment:** Upon receiving a high-confidence malware alert from the SIEM/EDR, automatically trigger a playbook to isolate the affected endpoint from the network to prevent lateral movement.
- **Credential Compromise Response:** When a compromised account is detected (e.g., through an impossible travel alert), automatically disable the account, terminate active sessions, and initiate a workflow for password reset and user notification.

For more nuanced incidents, the SOAR platform will serve as a case management and orchestration tool, automatically gathering relevant data from various systems and presenting it to a human analyst for a final decision, thereby streamlining the investigation process.

**Table 1: Recommended TCC Technology Stack**

| Capability Category | Technology Type | Key Functions | Integration Points |
|---|---|---|---|
| **Security Analytics** | Next-Gen SIEM | Centralized log collection, real-time correlation, threat detection, compliance reporting, UEBA. | EDR, NDR, Firewalls, Cloud Platforms, TIP, SOAR |
| **Automated Response** | SOAR | Automation of response playbooks, case management, security tool orchestration. | SIEM, EDR, TIP, Firewalls, Email Security |
| **Endpoint Security** | EDR / XDR | Deep visibility into endpoint activity, malware prevention, behavioral threat detection, remote response. | SIEM, SOAR, Forensics Tools |
| **Threat Intelligence** | TIP | Aggregation, analysis, and dissemination of threat intelligence from multiple sources. | SIEM, SOAR, Firewalls, EDR |
| **Network Security** | NDR | Analysis of network traffic for anomalous behavior and threats that bypass traditional controls. | SIEM, SOAR, Firewalls |
| **Vulnerability Mgmt.** | VM Platform | Network scanning, asset inventory, vulnerability identification, and risk-based prioritization. | EDR, Patch Management Systems |

# Part IV: Proactive Defense and Response: Specialized Operational Units

Beyond the 24/7 monitoring of the CTIC, the TCC must possess specialized, highly trained units capable of direct action—responding to major incidents, providing hands-on assistance to impacted entities, and conducting deep forensic analysis to understand and preempt future attacks.

## 4.1 Critical Incident Response Unit (CIRU)

House Bill 150 explicitly mandates the creation of a dedicated cybersecurity incident response unit.[5] This unit, designated here as the Critical Incident Response Unit (CIRU), will be the state's primary force for combating significant cyberattacks.

### Structure and Mission

The CIRU will be the TCC's elite team of incident responders, housed within the Directorate of Operations. It will be composed of a core cadre of full-time, dedicated experts in areas such as network security, endpoint analysis, and cloud incident response. During a large-scale incident, this core team will form the nucleus of a broader Computer Security Incident Response Team (CSIRT), augmented by specialists from the TCC's forensics lab, GRC directorate, and relevant partner agencies.[26] The CIRU's mission is to execute all phases of the incident response lifecycle as defined by frameworks like NIST and SANS: Preparation, Identification/Detection, Containment, Eradication, Recovery, and Lessons Learned.[26] This includes the authority and capability to perform "threat neutralization," such as removing malware, disabling unauthorized access, and patching critical vulnerabilities in real-time.[5]

### Rules of Engagement

A formal, pre-approved Incident Response Plan is critical to the CIRU's effectiveness. This plan must define clear incident severity levels, establish escalation protocols (including notification to the TCC Chief and the Governor's Office), and grant the CIRU the necessary authority to take decisive action on behalf of an impacted agency, such as disconnecting compromised systems from the network to prevent further damage. This plan must be regularly tested and refined through tabletop and full-scale operational exercises involving state and local partners.[27]

## 4.2 Field Remediation Teams (FRT)

Many local governments, school districts, and smaller state agencies lack the on-staff expertise to effectively manage the aftermath of a serious cyberattack. To bridge this capability gap, the TCC should establish regionally deployed Field Remediation Teams (FRTs). This model is based on the successful deployment of regional advisors by federal agencies like CISA and state-level teams like the California Cybersecurity Integration Center's (Cal-CSIC) response unit.[29]

### Mission and Deployment

The FRTs will serve as the TCC's deployable, "boots-on-the-ground" presence. Their mission is to provide direct, on-site technical assistance to public entities during and after a cyber incident. To ensure rapid response across Texas's vast geography, these teams should be strategically based in major hubs such as the Dallas-Fort Worth Metroplex, the Houston area, and the El Paso region. They would act as the TCC's forward-deployed liaisons, working directly with local IT staff, emergency managers, and law enforcement. Their services would include hands-on incident response support, assistance with vulnerability remediation, conducting post-incident security assessments to prevent recurrence, and helping entities recover and restore critical services.

### 4.3 The Digital Forensics Laboratory

HB 150 mandates the creation of a Digital Forensics Laboratory to support incident response and conduct proactive analysis.[2] This lab must be more than a traditional law enforcement evidence processing center; it must be a hub of deep technical analysis and threat discovery.

#### Capabilities and Dual Mandate

The lab must be equipped with industry-standard forensic tools for evidence acquisition and analysis from a wide range of devices, including servers, workstations, mobile phones, and cloud environments.[31] It must maintain an impeccable chain of custody for all evidence to ensure its integrity for potential legal proceedings.[28]

Crucially, the lab operates under a dual mandate that can create operational friction. It must support the CIRU's incident response mission, which prioritizes speed, containment, and service restoration. Simultaneously, it must support potential criminal investigations, which prioritize meticulous evidence preservation and attribution.[32] These priorities can conflict; for example, the fastest way to restore a service might be to wipe and rebuild a server, which would destroy the forensic evidence needed for prosecution. To manage this, the TCC must develop a clear "forensic triage" protocol in consultation with legal counsel and law enforcement partners. At the outset of an incident, this protocol will be used to determine the primary objective—restoration or prosecution—which will then dictate the specific forensic procedures to be followed.

#### Proactive Mission and Structural Model

Beyond reactive analysis, the lab is tasked with a proactive mission: developing and sharing cyber threat hunting tools and procedures to help entities proactively discover latent intrusions.[5] This involves reverse-engineering new malware samples, analyzing attacker techniques, and translating those findings into new detection rules for the statewide SIEM. To maximize its reach, the TCC could adopt a hub-and-spoke model similar to Indiana's High-Tech Crime Units.[31] The central lab in San Antonio would serve as the "hub" with the most advanced capabilities, supporting and collaborating with smaller regional "spoke" labs within major local law enforcement agencies, creating a powerful statewide network for forensic analysis and expertise.

## Part V: Service Delivery and Financial Sustainability

The long-term success of the TCC will depend on its ability to deliver valuable services to a diverse constituency and to build a sustainable financial model that balances its direct state appropriation with its legislative mandate for cost recovery.

### 5.1 Service Catalog and Consumption Model

A clearly defined service catalog is essential for communicating the TCC's value proposition and managing stakeholder expectations. A tiered model is recommended to differentiate between foundational services provided as a public good and advanced services offered on a cost-recovery basis.

- **Tier 0 (Public Good - Mandatory):** These are services provided to all Texans, funded entirely by direct appropriation. This includes the TCC's public cybersecurity awareness campaigns and the operation of the 24/7 statewide cybersecurity incident reporting hotline.[5]
- **Tier 1 (Core Services - Mandatory for Public Entities):** This tier represents the baseline of cybersecurity services required for all state agencies, institutions of higher education, and local governments to ensure a minimum standard of security across the state. These services, funded by direct appropriation, include the receipt of TCC threat intelligence bulletins and alerts, access to the state-mandated cybersecurity training programs, and adherence to the minimum security standards established by the TCC.[4]
- **Tier 2 (Advanced Services - Optional/Fee-for-Service):** This tier consists of a suite of advanced, resource-intensive services that public entities can choose to procure from the TCC on a cost-recovery basis.[5] This opt-in model allows the TCC to provide high-end capabilities without imposing unfunded mandates, a frequent source of friction between state and local governments.[34] Services in this tier could include:
    - **Managed SIEM:** Full ingestion and 24/7 monitoring of an entity's logs within the TCC's statewide SIEM platform.
    - **Managed Endpoint Detection and Response (EDR):** Provisioning and management of advanced EDR agents on an entity's endpoints.
    - **Advanced Security Assessments:** In-depth services like penetration testing, red team exercises, and application security reviews.
    - **Incident Response Retainer:** Guaranteed, priority access to the CIRU and

Field Remediation Teams.

While making Tier 1 services mandatory is crucial for establishing a statewide security baseline, lessons from other states, such as New York, show that such mandates are most effective when paired with state-provided resources, like free training materials, to help local entities comply.[35]

### 5.2 Comparative Analysis: The Texas Centralized Model vs. The Louisiana Partnership Model

The user query specifically requested a comparison with Louisiana's approach to cybersecurity. While Texas has chosen a centralized, state-agency-led model, Louisiana has pursued a more decentralized, partnership-driven model coordinated through a Cybersecurity Commission and heavily reliant on academic and federal partnerships.[36] Understanding the differences is key to appreciating the strategic choices embedded in the TCC's design.

**Table 2: Comparative Analysis of State Cybersecurity Models: Texas vs. Louisiana**

| Feature | Texas Cyber Command (TCC) | Louisiana (Cyber Command) |
|---|---|---|
| **Governance Structure** | Centralized state agency, a component institution of the UT System.[4] | Statewide advisory commission and university-led public-private partnerships.[36] |
| **Authority** | Formal rulemaking and enforcement authority over all public governmental bodies.[4] | Primarily advisory and collaborative; direct enforcement power resides with the Governor.[36] |
| **Funding Model** | Large direct state appropriation ($135M) combined with a legislative mandate for cost-recovery.[3] | Relies on a mix of federal grants (from CISA/DHS), direct partner funding, and industry collaboration.[37] |
| **Primary Focus** | Comprehensive "Whole-of-State" protection for all public sector IT and opt-in critical infrastructure.[4] | Strong initial focus on securing Operational Technology (OT) within the state's Executive Branch, critical energy, and chemical sectors.[37] |
| **Key Strengths** | Clear command structure, ability to enforce standards uniformly, economies of scale in technology procurement, unified incident response. | High degree of agility, deep integration with specific industry sectors (e.g., energy), effectively leverages partner funding, specialized expertise in OT security. |
| **Potential Challenges** | Risk of bureaucratic inertia, potential to alienate partners who prefer collaboration over top-down direction, long-term funding sustainability after initial appropriation. | Potential for a fragmented or uncoordinated response during a statewide crisis, reliance on the priorities of external partners, difficulty in enforcing baseline standards. |

This comparison highlights that Texas's model prioritizes unity of command and the ability to enforce a statewide security baseline. Louisiana's model prioritizes agility and deep, sector-specific collaboration. The TCC's challenge will be to leverage the strengths of its centralized structure while building the strong, trust-based partnerships that characterize the Louisiana model, particularly with its voluntary critical infrastructure partners.

### 5.3 A Hybrid Funding Strategy

The TCC's financial framework is defined by two key legislative provisions: a historic initial appropriation of $135 million and a mandate for cost recovery.[3] This requires a sophisticated hybrid funding strategy to ensure both immediate operational capability and long-term sustainability.

#### Balancing Appropriation and Cost Recovery

The initial $135 million appropriation should be strategically allocated to fund the TCC's foundational build-out (Phase 1 of the roadmap), including capital expenditures for technology and facilities, and the hiring of initial staff. Critically, this appropriation should also fully cover the ongoing operational costs of the mandatory Tier 0 and Tier 1 services provided to all public entities. This approach aligns with NASCIO's recommendation that states use general funds for core, universally needed infrastructure and security services.[40]

The cost-recovery mandate should be applied exclusively to the optional, Tier 2 advanced services. The TCC must develop a transparent and defensible pricing model for these services. The legislative language "when reasonable and practical" [5] suggests that the goal is not profit, but sustainability. Therefore, pricing should be based on a non-profit, at-cost principle. This ensures services remain accessible and avoids the perception that the TCC is competing with private sector cybersecurity firms. This market-like mechanism also serves a strategic purpose: it forces the TCC to continuously demonstrate the value of its services in a way that entities are willing to pay for, instilling a culture of customer focus and service excellence.

### Aggressively Pursuing Federal Grants

The TCC should establish a dedicated grant-writing and management function to aggressively pursue federal funding opportunities. Programs like the DHS/FEMA State and Local Cybersecurity Grant Program (SLCGP) are specifically designed to help states fund these types of initiatives.[41] Securing these grants can supplement the state appropriation, reduce the financial burden on local governments by helping them meet matching requirements, and provide pass-through funding for local cybersecurity projects, further strengthening the "Whole-of-State" ecosystem.[43]

## Part VI: Phased Implementation Roadmap

Translating this strategic blueprint into an operational reality requires a disciplined, phased implementation plan. The following roadmap breaks down the monumental task of building the TCC into three distinct phases over 36+ months, with clear objectives, activities, and success metrics for each. This provides a clear path to achieving Full Operational Capability (FOC) and allows for effective oversight and resource allocation. The initial 18-month timeline for the TCC to become operational serves as the foundation for Phase 1.[2]

### TCC Implementation Roadmap

#### Phase 1: Foundational Build-Out & Initial Operational Capability (IOC)

- Timeframe: Months 0-18
- Key Objectives: Establish leadership and core staff; define foundational governance; procure and deploy core technology; launch 24/7 intelligence center.
- Major Activities:
    - Appoint and confirm Chief and key directors.
    - Hire initial 65 staff, focusing on leadership and platform engineering.
    - Finalize MOU with UT System defining operational independence.
    - Establish Technical and Workforce Advisory Councils.
    - Procure and deploy statewide SIEM, EDR, and TIP platforms.
    - Stand up the 24/7 Cyber Threat Intelligence Center (CTIC) and incident hotline.
    - Develop and publish initial Data Privacy and Incident Response policies.
- Success Metrics:
    - TCC leadership team is fully staffed.
    - 90% of initial 65 positions are filled.
    - Core technology platforms are deployed and ingesting security data from 100% of executive branch state agencies.
    - CTIC is operating 24/7 and processing incident reports.

**Phase 2: Operational Expansion & Service Rollout**

- Timeframe: Months 18-36
- Key Objectives: Expand services to local governments; operationalize response teams; mature the financial model.
- Major Activities:
    - Staff and deploy regional Field Remediation Teams.
    - Procure and implement SOAR platform; develop and deploy initial 50+ automated response playbooks.
    - Onboard the first cohort of local governments and school districts into TCC services.
    - Launch the formal Tier 2 service catalog and begin cost-recovery operations.
    - Conduct the first annual, full-scale statewide cyber exercise.
- Success Metrics:
    - All Field Remediation Teams are staffed and have achieved operational readiness.
    - Measurable reduction in Mean Time to Respond (MTTR) for common incidents due to SOAR automation.
    - At least 25% of Texas counties and 25% of large school districts are consuming at least one TCC service.
    - Cost-recovery revenue meets 100% of initial projections.

**Phase 3: Full Operational Capability (FOC) & National Leadership**

- Timeframe: Months 36+
- Key Objectives: Achieve a mature, proactive security posture; establish Texas as a national leader in cybersecurity innovation and workforce development.
- Major Activities:
    - Implement advanced, proactive threat hunting programs within the Digital Forensics Lab.
    - Achieve deep integration and bidirectional intelligence sharing with all major critical infrastructure sectors in Texas.
    - The UTSA-TCC workforce pipeline is fully operational, meeting or exceeding annual hiring needs.
    - Host a national summit on state-level cybersecurity policy and operations.
    - Publish an annual, public "State of Cybersecurity in Texas" report.

- Success Metrics:
    - TCC is formally recognized by federal partners (CISA, NSA) and national organizations (NASCIO, NGA) as a model for state cybersecurity.
    - A statistically significant, year-over-year reduction in successful major cyberattacks against Texas public entities.
    - TCC becomes a net exporter of cybersecurity talent and best practices to other states and the private sector.

## Conclusion: Securing the Future of Texas

The creation of the Texas Cyber Command is the state's most significant and decisive action to date in confronting the escalating threats of the digital age. The challenges are immense, but the opportunity is even greater. By adopting the "Whole-of-Ecosystem" approach outlined in this blueprint, the TCC can harness the combined strength of its public, private, academic, and federal partners to build a defensive shield that is greater than the sum of its parts.

Success requires more than just technology and funding; it demands a new way of thinking about cybersecurity as a shared, statewide responsibility. It requires building bridges of trust with hundreds of local governments and critical infrastructure operators. It demands a relentless focus on developing the next generation of cyber defenders through a revolutionary partnership with the UT System. And it requires unwavering executive and legislative support to see this multi-year mission through to completion.

The roadmap is clear. The resources have been allocated. By executing this strategy with discipline, transparency, and a spirit of true partnership, the Texas Cyber Command will not only fulfill its legislative mandate to protect the state's vital digital assets but will also forge a new national standard for cybersecurity, sending a clear message to adversaries around the globe: Don't Mess with Texas.

**Works cited**


1. Governor Abbott Signs Texas Cyber Command Into Law In San Antonio, accessed August 6, 2025, https://gov.texas.gov/news/post/governor-abbott-signs-texas-cyber-command-into-law-in-san-antonio
2. Texas governor signs bill for statewide Cyber Command | StateScoop, accessed August 6, 2025, https://statescoop.com/texas-cyber-command-gov-abbott/
3. Texas Cyber Command becomes law, UTSA to play key role, accessed August 6, 2025, https://www.utsa.edu/today/2025/06/story/abbott-signs-texas-cyber-command-into-law.html
4. Texas Cyber Command: New Authority for Statewide Cybersecurity ..., accessed August 6, 2025, https://www.pillsburylaw.com/en/news-and-insights/texas-cyber-command-cybersecurity.html
5. capitol.texas.gov, accessed August 6, 2025, https://capitol.texas.gov/tlodocs/89R/analysis/html/HB00150E.htm
6. Texas Launches Cyber Command – Tan Parker, accessed August 6, 2025, https://www.tanparker.com/texas-launches-cyber-command/
7. HB 150 - 89th Legislature - Texas Policy Research, accessed August 6, 2025, https://www.texaspolicyresearch.com/bills/89th-legislature-hb-150/
8. The Whole of State Approach: SafeguardIng Our Digital Communities - Rubrik, accessed August 6, 2025, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/whole-of-state-approach-wp.pdf
9. Top considerations for adopting a whole-of-state cybersecurity strategy - Route Fifty, accessed August 6, 2025, https://www.route-fifty.com/cybersecurity/2025/03/top-considerations-adopting-whole-state-cybersecurity-strategy/403450/
10. Whole-of-State Cybersecurity Gains Ground in Government - GovTech, accessed August 6, 2025, https://www.govtech.com/security/whole-of-state-cybersecurity-gains-ground-in-government
11. Public Sector Whole-of-State Cybersecurity - CrowdStrike, accessed August 6, 2025, https://www.crowdstrike.com/en-us/solutions/state-local-government/whole-of-state-cybersecurity/
12. Whole-of-state cybersecurity: How to implement and build a sustainable program - AWS, accessed August 6, 2025, https://aws.amazon.com/blogs/publicsector/whole-of-state-cybersecurity-implement-build-sustainable-program/
13. About | Virginia IT Agency, accessed August 6, 2025, https://www.vita.virginia.gov/about/organization/
14. Organizational Chart - Virginia IT Agency, accessed August 6, 2025,

https://www.vita.virginia.gov/about/organization/org-chart/
15. Securing States - NASCIO, accessed August 6, 2025, https://www.nascio.org/resource-center/securing-states/
16. Securing States: Modernizing to Attract & Retain Cyber Talent - NASCIO, accessed August 6, 2025, https://www.nascio.org/resource-center/resources/securing-states-modernizing-to-attract-retain-cyber-talent/
17. 2025 State CIO TOP 10 Priorities | NASCIO, accessed August 6, 2025, https://www.nascio.org/wp-content/uploads/2024/12/NASCIO-2025-State-CIO-Top-10-Priorities.pdf
18. Cybersecurity education and workforce development | NIST, accessed August 6, 2025, https://www.nist.gov/cybersecurity-education-and-workforce-development
19. Louisiana State Police Partners with LSU to Solve Critical Challenges in Industrial Cyber, accessed August 6, 2025, https://www.lsu.edu/mediacenter/news/2023/09/wfl-ics.php
20. A Compact to Improve State Cybersecurity - IN.gov, accessed August 6, 2025, https://www.in.gov/cybersecurity/files/NGA-Cyber-Compact.pdf
21. Cybersecurity Credentialing and Education Resources - National Governors Association, accessed August 6, 2025, https://www.nga.org/projects/cybersecurity-credentialing-and-education-resources/
22. Security Information & Event Management (SIEM) - CrowdStrike, accessed August 6, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/security-information-and-event-management-siem/
23. SIEM Use Cases: Top 10 Use Cases - SentinelOne, accessed August 6, 2025, https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-use-cases/
24. Implementing SIEM and SOAR platforms: Practitioner guidance | Cyber.gov.au, accessed August 6, 2025, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/implementing-siem-and-soar-platforms/implementing-siem-and-soar-platforms-practitioner-guidance
25. Top 10 SIEM Use Cases Today: Real Examples and Business Value - Splunk, accessed August 6, 2025, https://www.splunk.com/en_us/blog/learn/siem-use-cases.html
26. Incident Response Plan: Frameworks and Steps - CrowdStrike, accessed August 6, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/
27. Build: A cyber security incident response team (CSIRT) - NCSC.GOV.UK, accessed August 6, 2025, https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team

28. What Is CSIRT? The Computer Security Incident Response Team Complete Guide - Splunk, accessed August 6, 2025, https://www.splunk.com/en_us/blog/learn/csirt-computer-security-incident-response-team.html
29. CISA Regions, accessed August 6, 2025, https://www.cisa.gov/about/regions
30. California Cybersecurity Integration Center's (Cal-CSIC), accessed August 6, 2025, https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/
31. High-Tech Crime Unit Program - Indiana, accessed August 6, 2025, https://www.in.gov/ipac/high-tech-crime-unit-program/
32. Forensics — LE - FBI.gov, accessed August 6, 2025, https://le.fbi.gov/science-and-lab/forensics
33. Forensic Expertise - Secret Service, accessed August 6, 2025, https://www.secretservice.gov/investigations/forensic
34. Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers - NASCIO, accessed August 6, 2025, https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf
35. New York's Cybersecurity Overhaul: What Municipalities and Nonprofits Need to Know, accessed August 6, 2025, https://hedgemanlaw.com/new-yorks-cybersecurity-overhaul-what-municipalities-and-nonprofits-need-to-know/
36. Cybersecurity Incident Resources | Office of Governor Jeff Landry, accessed August 6, 2025, https://gov.louisiana.gov/page/cybersecurity-incident-resources-
37. LSU partners with CISA, DHS, and INL to launch critical ..., accessed August 6, 2025, https://industrialcyber.co/news/lsu-partners-with-cisa-dhs-and-inl-to-launch-critical-infrastructure-cybersecurity-model/
38. CISA, DHS S&T, INL, LSU Help Energy Industry Partners Strengthen Incident Response and OT Cybersecurity, accessed August 6, 2025, https://www.cisa.gov/news-events/news/cisa-dhs-st-inl-lsu-help-energy-industry-partners-strengthen-incident-response-and-ot-cybersecurity
39. CISA, DHS, INL host LSU to strengthen cyber defense training across critical infrastructure sector, accessed August 6, 2025, https://industrialcyber.co/training-development/cisa-dhs-inl-host-lsu-to-strengthen-cyber-defense-training-across-critical-infrastructure-sector/
40. The 2023 State CIO Survey | NASCIO, accessed August 6, 2025, https://www.nascio.org/wp-content/uploads/2023/09/NASCIO_2023-State-CIO-Survey-A.pdf
41. State and Local Cybersecurity Grant Program | FEMA.gov, accessed August 6, 2025, https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program
42. DHS Launches Over $100 Million in Funding to Strengthen Communities' Cyber

Defenses, accessed August 6, 2025, https://www.cisa.gov/news-events/news/dhs-launches-over-100-million-funding-strengthen-communities-cyber-defenses
43. New state, local cyber grant rules prohibit spending on MS-ISAC | StateScoop, accessed August 6, 2025, https://statescoop.com/state-local-cyber-grant-msisac-2025/
44. Ensure Responsible Implementation of the State and Local Cybersecurity Grant Program - NASCIO, accessed August 6, 2025, https://www.nascio.org/wp-content/uploads/2024/01/NASCIO-Advocacy-Priorities-2024-cybersecurity-grant-a.pdf