Legislative Appropriations Request

for Fiscal Years 2028 and 2029

Submitted to the

Office of the Governor, Budget and Policy Division,

and the Legislative Budget Board

by

TXCC

TEXAS CYBER COMMAND

This Page Intentionally Left Blank

Legislative Appropriations Request

for Fiscal Years 2028 and 2029

PREVENT★SECURE★PROTECT★DEFEND★EDUCATE

Submitted to the

Office of the Governor, Budget and Policy Division,

and the Legislative Budget Board

by

Texas Cyber Command

Table of Contents

Administrator's Statement

Introduction

Texas Cyber Command (TXCC) submits this Administrator's Statement in support of its FY28–29 Legislative Appropriations Request (LAR). This is the Command's first request for a full biennium of operations after TXCC was established as an independent agency in Texas Government Code (TGC) 2063.

In creating TXCC, both the Governor and Legislature recognized that the frequency, scale, and sophistication of cyber incidents targeting Texas government systems and critical infrastructure, coupled with the state's dependence on the Internet, had outgrown a model in which cybersecurity was one function among many at a general-purpose technology agency.
TXCC became operational in March 2026 and is completing the transfer of specified cybersecurity and network-security functions, personnel, contracts, property, records, and appropriated funds from the Department of Information Resources (DIR).

This LAR includes the base budget for the build-out of statutorily required capabilities across the FY28-29 biennium, as well as the Command's request for Exceptional Items.

Agency Statutory Mission and Mandate

Texas is critical to our economic prosperity and national defense. Texas is the eighth-largest economy in the world and a global leader in energy production. Texas is home to critical military installations, and a national transportation hub featuring important ports, airports, and rail lines. These strengths also make Texas a prime target for nation-state cyber actors, criminal ransomware groups, and hacktivist collectives. Cyber threats are moving faster, adversaries are more capable, advanced technologies are increasing both the scale and impact of attacks and disruption. At the same time, Texas's dependency on – and vulnerability in – cyberspace is near absolute, making the security and resilience of our digital and critical infrastructure essential to the state's continued prosperity and security. The threat has outgrown a traditional approach to cybersecurity.

Thus, the Legislature established and funded Texas Cyber Command as a dedicated, mission-focused organization with the singular responsibility to defend Texas, strengthen the resilience of its critical infrastructure, and protect the systems on which Texans depend.

Mission

TXCC's mission is to prevent and respond to cybersecurity incidents that affect state governmental entities and critical infrastructure in Texas.

Vision

TXCC's vision is a Texas where Texans are safe in the digital world and trust that the essential services they depend on are secure; a Texas that leads the nation in cyber readiness and resilience.

TXCC will achieve this vision by leading a coordinated statewide security program that turns threat intelligence into prevention, strengthens common standards and services, expands workforce capacity, reinforces public trust, and protects Texas's data and critical systems within the authorities granted by law. TXCC is building the people, processes, partnerships, and technologies needed to strengthen Texas's ability to anticipate cyber threats, secure, protect, and defend critical information technology (IT) and operational technology (OT) networks, sustain essential public services online, and facilitate cybersecurity training to state agencies and covered entities.

TXCC executes its mission across six operational terrains, a framework that mirrors the U.S. Department of War's approach to organizing mission, functions, and tasks across distinct operational environments. This framework aligns TXCC's responsibilities with the major constituencies identified in TGC 2063 and provides a clear structure for executing its statewide mission. The fundamental principle is simple: you cannot secure, protect, and defend what you cannot see. These operational terrains represent the networks, systems, and environments over which TXCC must establish visibility, understand risk, and build the capability to secure, protect, and defend Texas. The six operational terrains include:

1. **Texas State Government Entities.** Departments, commissions, boards, offices, or other agencies in the executive branch of state government that was created by the constitution or a statute.
2. **Institutions of Higher Education**. The university system and institutions of higher education, as defined by Section 61.003, Education Code.
3. **Law Enforcement and Judiciary**. The supreme court, the court of criminal appeals, courts of appeals, district courts, the Texas Judicial Council, and other agencies in the judicial branch of state government.
4. **Covered Entities**. Private entities operating in critical infrastructure or a local government with which TXCC contracts to provide cybersecurity services.
5. **Critical Infrastructure**. Infrastructure in Texas that is vital to the security, governance, public health and safety, economy, and morale of the state or the nation.
6. **Texas's Data**. Data held by the entities listed above.

TXCC's strategic direction is to shift the state's cyber posture from primarily reactive incident response toward proactive prevention resulting from enhanced readiness and increased resilience across these six operational terrains. TXCC will prioritize cyber threat intelligence, common operational capabilities, scalable standards and services, early risk identification, threat-informed protective actions, exercises, and workforce development that help stop incidents before they disrupt Texas government services or critical infrastructure.

The Command established four goals in the Strategic Plan submitted to the Legislature on June 1, 2026:

A. Enhance Texas's cybersecurity readiness
B. Boost the State of Texas's cyber resilience
C. Catalyze growth in Texas's highly skilled cybersecurity workforce
D. Indirect administration

The Command will accomplish these goals through its workforce and five core capabilities that TGC 2063 directs the Command to build and operate:

1. A Cyber Threat Intelligence Center (CTIC)
2. A Cybersecurity Incident Response Unit (CIRU)
3. A Security Operations Center (SOC)

4. A statewide Information Sharing and Analysis Organization (ISAO)
5. A Digital Forensics Laboratory (DFL)

Baseline Request and Program Identified as an Exception to the Baseline Limitation

The Policy Letter accompanying the FY28–29 LAR instructions limits most agencies' General Revenue and General Revenue–Dedicated baseline requests to amounts approved by the Legislative Budget Board and the Governor's Office of Budget and Policy. TXCC's baseline request is an exception to that limitation because its 2026–2027 appropriation does not reflect a fully phased-in operating level from which a standard baseline can be derived. A standard baseline assumes that the current biennium's appropriation is sufficient to sustain existing programs, staffing, and service levels into the next biennium. That assumption does not apply to TXCC. The agency is less than eighteen months old, was activated only six months before entering the LAR process, continues to absorb functions and personnel transferred from another agency, and is building statutorily mandated capabilities that were neither fully staffed nor operational at the beginning of the 2026–27 biennium. TXCC's current appropriation is not a mature operating baseline; it is the foundation for establishing the statewide cybersecurity capability the Legislature created TXCC to deliver. The FY 2028–29 request is necessary to complete that build-out, fully establish the personnel and capabilities required by statute. This request is targeted investment required to fully operationalize the capability the Legislature established. TXCC approaches this request with discipline and a clear commitment to fiscal stewardship. The LAR is designed to provide the resources necessary to execute TXCC's statutory responsibilities while maintaining operational efficiency, transparency, accountability, and responsible stewardship of taxpayer dollars. TXCC is committed to maximizing the cybersecurity value of every dollar entrusted to the agency and to delivering the statewide capability, security, and resilience the Legislature established TXCC to provide.

Funding for FY27. TXCC's FY27 budget was determined by the transfer of FY26-27 cybersecurity funding from DIR and an additional allocation of funds appropriated by the Legislature. Together TXCC's FY27 topline budget is $122,433,128.

The FY28–29 baseline request. TXCC's FY28–29 LAR is $243,397,595. This includes the cost of operating the Command at its statutorily authorized capacity of 84 full-time-equivalent positions (FTEs), inclusive of cybersecurity personnel transferred from DIR, as well as the 3% reduction guidance entering into Texas 90th Legislative Session.

Allocation of the FY28-29 baseline request. TXCC has allocated its request for FY28-29 to the mission, responsibilities, general powers, and duties assigned to TXCC in TGC 2063. This request also accounts for missions, functions, and tasks codified in TGC 2054 and 2059. The baseline request aims to fulfill as many of these functions as effectively as possible within the prescribed baseline. These include, for example, staffing and operating the CTIC, ISAO, SOC, CIRU, and DFL. It also includes identifying cyber threats to critical infrastructure and state systems, monitoring and coordinating cyber threat intelligence and information systems to detect and warn entities of cyberattacks, providing tools to enhance cybersecurity defenses, planning and executing cybersecurity incident response, conducting digital forensics of cybersecurity incidents, facilitating cybersecurity workforce education and training, and creating partnerships necessary to effectively carry out the Command's functions.

As outlined in TXCC's Strategic Plan Fiscal Years 2027-2031, TXCC is shifting its mission toward preventing cybersecurity incidents before they impact state government and critical infrastructure, rather than relying on responding after an incident occurs. This prevention-focused approach has informed the development of the FY 2028-29 baseline and prioritizes investments that reduce risk, strengthen readiness, and improve statewide resilience.

Significant Changes in Policy

The most significant policy change reflected in this request is the one already enacted by the Legislature: the shift from a fragmented model of state cybersecurity, in which DIR administered a security system on behalf of participating entities, to a centralized model in which a single, statutorily independent command is responsible for statewide cyber threat intelligence and detection, incident prevention and response, information sharing, and coordination. The FY28–29 LAR is the first request to reflect a full biennium of the new model.

Significant Changes in Provision of Service

Mission stakeholders. In TXCC's Strategic Plan for Fiscal Years 2027-2031, TXCC makes a clear distinction that it does not operate through traditional customer transactions. Instead, the Command works with mission stakeholders, partners, and teammates to achieve statewide cybersecurity outcomes. TXCC's mission stakeholder community is substantially broader than the former DIR network security program. Pursuant to TGC 2063, the Command's mission spans six operational terrains:

state government, institutions of higher education, law enforcement and the judiciary, covered entities such as participating local governments and school districts, critical infrastructure, and Texas's data. As the Command completes its stand-up and Texas's Regional Security Operations Centers (RSOCs) and Virtual Incident Response Team (VIRT) mature, the number and diversity of entities receiving coordinated cybersecurity support and defense will continue to expand.

Cost and efficiency. Consolidating cybersecurity functions into a single agency creates efficiencies of scale, reduces duplication, and strengthens statewide service delivery that was not achievable when capabilities were distributed across multiple agencies. For example, TXCC can negotiate threat-intelligence, managed-detection, and other cybersecurity services at statewide scale, operate a single digital forensics capability rather than duplicative programs, and deploy consistent, reliable incident-response processes across state government. Centralization also improves interoperability, reduces administrative and technology overlap, and allows specialized expertise and shared services to be deployed where risk is greatest. These efficiencies will increase as TXCC reaches its authorized 84-FTE capacity, RSOCs and VIRT mature, and contracted services transition to statewide scale. The result is greater cybersecurity capability per dollar, reduced duplication, stronger operational consistency, and a more effective statewide defense posture.

Technology. The Command's work depends on investing in capabilities that either did not exist in Texas government before 2025 or existed only in limited, fragmented form. These include a comprehensive cyber threat intelligence and warning capability, an expanded statewide Information Sharing and Analysis Organization, enhanced capabilities to detect, analyze, respond to, and mitigate cyber intrusions across state government and participating covered entities, a centralized incident-reporting portal, and a dedicated digital forensics capability for evidentiary-quality investigations. These capabilities establish the statewide cybersecurity infrastructure necessary to execute TXCC's statutory mission, strengthen Texas's ability to prevent, detect, and disrupt cyber threats before they compromise critical systems and services, and deliver a more coordinated, resilient, and defensible statewide cybersecurity posture.

Privatization. The Command leverages private-industry expertise and commercial capabilities to rapidly scale specialized cybersecurity capacity, including threat-intelligence feeds, managed detection and response, and specialized forensic tools and services. This approach allows TXCC to access capabilities, technology, and expertise that would be costly and time-consuming to build entirely with state employees during the agency's early operating years. Engagement with private industry also provides access to specialized expertise, rapidly evolving technologies, and the ability to scale capabilities

quickly as mission demands change. As the agency matures, the balance between state personnel and private-industry support will continue to evolve, but private-industry engagement will remain an important component of the Command's operating model during the FY 2028-29 biennium.

Significant Externalities

Population growth and a widening attack surface. Texas's population reached approximately 31.7 million residents in 2025, an increase of roughly 391,000 residents in a single year and approximately 2.6 million residents since 2020, more than any other state added over that period. Each new resident interacts with state and local government through an increasing number of digital services and connected devices, from driver's licenses and vehicle registrations to hunting and fishing licenses, benefits eligibility, and court records. Every one of those digital touchpoints, and every device connected to the networks that support them, is a potential entry point for a cyber attack.

As Texas's population grows, so does its dependence on critical services such as water and wastewater, power, telecommunications and transportation. These services are highly interconnected and power Texas's modern economy. As such, they represent additional vulnerable attack surfaces that must be protected.

The Command's workload is a direct function of this growth: more residents, more connected endpoints, more transactions, more demand for critical services, and more attack surface across state and local government systems and critical infrastructure entities that TXCC is charged with helping to defend.

Cyber threats to Texas networks. The need for a centralized cybersecurity organization is not theoretical. In early 2024, a pro-Russian hacktivist group compromised the industrial control system of the water utility serving Muleshoe, Texas, causing a water storage tank to overflow. In the same period, a ransomware attack on UT Health East Texas compromised the private health information of more than 15,000 Texans. Legislative testimony during consideration of the Command's enabling legislation cited data breaches that compromised the personal information of more than 15 million Texans in 2024 alone.

Most recently, in June 2026, TXCC detected and helped scope a data breach at a vendor serving the Texas Parks and Wildlife Department, which exposed the driver's license numbers, passport numbers, and contact information of more than three

million Texas hunting and fishing license holders. That incident is a concrete demonstration of the growing demand for detection and incident response capability this request funds.

Finally, the new pacing threat to networks is the advent of artificial intelligence (AI) models and autonomous agents able to identify previously unknown software vulnerabilities (also called "zero days") and develop exploits at a previously unimaginable pace gives heightened urgency to the mission.

While AI is at the forefront right now, Texas must also anticipate the emergence of a quantum computer. An effective quantum computer will render much of the Internet's current data encryption and identity management schemes obsolete. This shift will have profound implications for Internet security and cybersecurity.

A shifting federal posture. Federal cybersecurity policy has increasingly placed operational and budgetary responsibility for defending state and local government systems, and the critical infrastructure that depends on them, on the states themselves, rather than relying primarily on federal agencies to provide cyber defenses. TXCC does not anticipate any change in federal direction on this front in the near-term.

Workforce demand. Qualified cybersecurity professionals are in high demand across the nation. TXCC's continued partnership with UTSA and other Texas institutions of higher education, through the formation of an Academic Alliance, is intended to mitigate this challenge and facilitate the growth of a highly skilled cybersecurity workforce that Texas will need to secure its future in cyberspace.

Exceptional Items

TXCC is submitting seven Exceptional Items for additional funding beyond the FY28-29 LAR baseline. Each is directly tied to fulfilling TXCC's statutory mandate and expectations the Legislature established for the Command in TGC 2063. These Exceptional Items are as follows:

1. **Sustain Statewide Cybersecurity Services Transferred from DIR and Cost Recovery Funding.** When the Legislature created TXCC, responsibility for two existing statewide cybersecurity strategies (C.1.1 – Security Policy & Awareness and C.1.2 – Security Services) transferred from DIR to TXCC. These strategies were supported by General Revenue and cost-recovery funding. While responsibility for these services transferred to TXCC, the funding necessary to fully sustain these services did not. TXCC is requesting General Revenue to replace the cost-recovery funding previously used by DIR so that TXCC can continue delivery of these statewide cybersecurity services. This Exceptional Item would restore that funding.

2. **TXCC Staffing to Implement Statutory Cybersecurity Responsibilities.** TXCC requests 120 additional FTEs to implement and sustain the statewide cybersecurity mission envisioned in TGC 2063. The additional FTEs will expand threat analysis and warning; 24-hour incident report intake, coordination, response, and recovery; digital evidence and forensic support; security operations; information sharing; standards, training, readiness, and assurance; partnerships; and the legal, financial, procurement, human resources, technology, communications, project management, and administrative controls required for accountable execution.

3. **Securing AI and Preparing Texas for Quantum Risk.** Texas must prepare now for two technology shifts that could materially change the State's cybersecurity risk: artificial intelligence and the emergence of a quantum computer, which will render much of the Internet's current data encryption and identity management schemes obsolete. AI is rapidly expanding into defensive workflows, sensitive-data processing, and autonomous actions. This provides the opportunity to establish a governed statewide capability to discover, assess, test, secure, and responsibly deploy these technologies. Funding will create a statewide cryptographic inventory and transition program, including discovery, cryptographic bills of materials, risk sequencing, readiness assessments, standards, pilots, and training. This investment gives Texas a disciplined path to adopt emerging technology without sacrificing security, evidence, accountability, or operational control, strengthening capabilities while protecting Texas's sensitive data and critical services.

4. **ISAO: Information Sharing and Governance Modernization.** Under TGC 2063, TXCC Texas must operate at least one ISAO, a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share cybersecurity threats, best practices, and remediation strategies. Current records, contractor-

supported assessments, member onboarding, findings, remediation, and dissemination processes remain fragmented and manual. This Exceptional Item modernizes the ISAO and related governance and cloud-assurance workflows, allowing TXCC to fulfill the TGC 2063 vision of sharing cybersecurity information and analysis with mission stakeholders, partners, and teammates.

5. **CTIC: Faster Cyber Threat Warning for Texas Critical Infrastructure**. TGC 2063 assigns cyber threat intelligence functions to TXCC that include monitoring and coordination of cyber threat intelligence, detection and warning, identification of threats to state systems and critical infrastructure, administration of the statutory intelligence function, clearinghouse responsibilities, and strategic guidance for response. TXCC's baseline budget provides foundational capability but is ultimately insufficient. This Exceptional Item will strengthen Texas Cyber Command's ability to identify, analyze, and communicate cyber threats affecting state systems and critical infrastructure before those threats result in significant operational consequences.

6. **Rapid Cyber Incident Intake, Coordination, and Recovery.** TGC 2063 requires the Command to receive cyber incident reports, operate a 24-hour cyber reporting hotline for state agencies and covered entities, administer a statewide portal for cybersecurity incident management, and support entities experiencing incidents. Existing hotline, ticketing, collaboration, response, and partner channels do not maintain one tested record from first contact through assignment, response, evidence handoff, recovery, follow-up analysis, and closure. This Exceptional Item will close those gaps.

7. **Shared Cyber Protection for Texas Government, RSOCs and Partners.** TXCC must implement consistent identity, digital trust, edge, Domain Name Service (DNS), and cloud protections to execute the network-security and cybersecurity-service responsibilities envisioned in TGC 2063. This consistency is also required for setting standards across RSOCs, supporting the expansion of RSOCs in Texas, and their services provision. Existing entity identity systems, certificate services, network and DNS providers, cloud-native controls, enterprise agreements, and local practices provide uneven coverage and no common statewide service catalog, onboarding model, lifecycle control, telemetry interface, support model, or unit-cost basis. This Exceptional Item will close those key gaps.

Effects Of Legislation: House Bill 149 (89R) and House Bill 4751 (89R)

H.B. 149, 89th Leg., R.S, is the Texas Responsible Artificial Intelligence Governance Act (TRAIGA). Among other things, it directs DIR to create a regulatory sandbox program allowing companies to test innovative AI systems without obtaining a license, registration, or other regulatory authorization. TXCC recommends that it be tasked, but is currently not funded, to provide cybersecurity guardrails for this sandbox program to prevent AI model breakouts from the sandbox and to support DIR in the use of this sandbox by program participants for cybersecurity testing under the category of public services. The former issue is of concern, given recent reports of Large Language Models escaping private-sector sandboxes and autonomously conducting cyber intrusions on the Internet. DIR's AI sandbox program should guard against this risk.

H.B. 4751 89th Leg., R.S, established Texas's Quantum Initiative. Its aim is to position Texas as a leader in quantum computing, networking, and sensing. The advent of a quantum computer able to decrypt or otherwise break digital security techniques currently not achievable by classical computers will have significant implications for future Internet security. As the advisory committee on quantum established in HB 4751, TXCC believes the state of Texas will be better postured if TXCC is resourced to support this advisory committee and is directed to assist the committee in the formulation of the strategic plan for the development of the quantum economy in Texas.

TXCC estimates that five additional FTEs are necessary to effectively execute functions contemplated by HB 149 and HB 4751 and to fulfill the responsibilities envisioned by the Legislature.

Authority to Conduct Background Checks

TGC §2063.504 requires the Command to obtain a background screening for each individual serving as a member of the VIRT to provide rapid response assistance with TXCC.

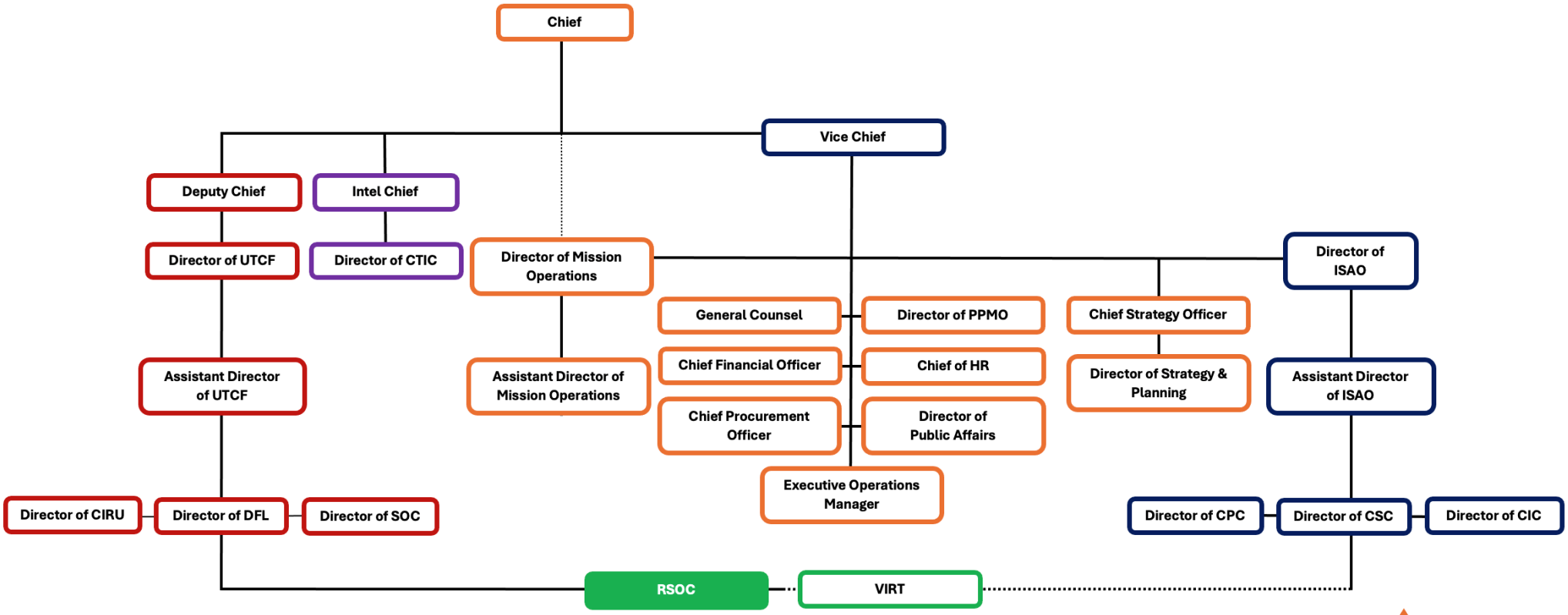
Conclusion

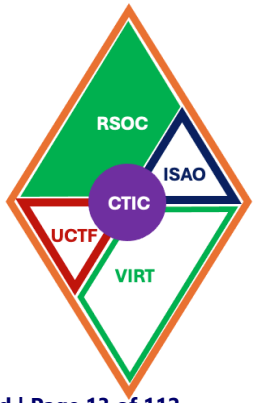
TXCC's FY28-29 LAR reflects the transition from a newly established legislative mandate to a fully operational, mission-focused statewide cybersecurity command. The request is presented as an exception to the standard baseline limitation because TXCC's first biennium appropriation supported initial stand-up, organizational transition, and capability development, rather than the recurring resources required to sustain the full scope of the Legislature's statutory mandates.

This LAR provides the resources necessary to complete that transition and establish the enduring statewide cybersecurity capability the Legislature created TXCC to deliver. TXCC approaches this request with discipline, accountability, and a commitment to responsible stewardship of state resources, with each requested investment directly tied to mission requirements and measurable statewide impact.

I appreciate the Legislative Budget Board's and the Governor's Office of Budget and Policy's consideration of this request. TXCC stands ready to provide any additional information necessary to support your review and to demonstrate how these resources will strengthen the security and resilience of Texas.

TEXAS CYBER COMMAND
EXECUTIVE ADMINISTRATION ORGANIZATION CHART





Description of Organizational Functions

Chief

The Chief of Texas Cyber Command serves as TXCC's chief executive and directs the strategy, policies, operations, and resources necessary to execute the Command's statutory responsibilities. The Chief leads Texas's statewide cybersecurity mission to prevent and respond to cyber threats, strengthen the security and resilience of state systems and critical infrastructure, coordinate cyber threat intelligence and incident response, advance trusted information sharing and partnerships, and develop the capabilities and workforce necessary to protect Texas against evolving cyber risks.

Vice Chief

The Vice Chief serves as the principal deputy to the Chief, assisting in the leadership, direction, and execution of TXCC's mission. The Vice Chief oversees Headquarters and the Information Sharing and Analysis Organization (ISAO), synchronizes activities across assigned functions, and ensures organizational priorities, resources, and initiatives remain aligned with the Command's statewide cybersecurity mission.

Deputy Chief

The Deputy Chief serves as TXCC's senior operational executive and technical advocate, leading coordinated statewide cybersecurity operations and overseeing the Unified Cyber Task Force, including the Security Operations Center, Cyber Incident Response Unit, and Digital Forensics Laboratory. The Deputy Chief is responsible for the technology ecosystem, performance, regional coordination, and the effective integration of personnel, capabilities, and resources across the Command's internal operational elements.

Intelligence Chief

The Intelligence Chief leads the agency's cyber threat intelligence activities, overseeing the collection, analysis, and dissemination of intelligence to support informed decision-making and cybersecurity operations. This role is expected to maintain Sensitive Compartmented Information (SCI) eligibility to enable direct interaction with United States government national security and intelligence organizations. The Intelligence Chief ensures timely threat information is shared with leadership and partners to identify emerging risks, improve situational awareness, and strengthen statewide cyber preparedness and response.

Director of Mission Operations

The Director of Mission Operations oversees the agency's administrative functions and coordinates activities across the executive office to ensure organizational priorities are effectively executed. The role supports the Chief and Vice Chief by managing executive operations, synchronizing activities across divisions, tracking major initiatives and leadership decisions, resolving coordination issues, and ensuring senior leaders have the information, alignment, and follow-through necessary to advance the Command's mission.

Assistant Director of Mission Operations

The Assistant Director of Mission Operations serves as the principal deputy to the Director of Mission Operations, supporting the coordination and execution of executive priorities across TXCC. The role tracks key initiatives and leadership decisions, coordinates across divisions, prepares executive materials, manages follow-through on action items and commitments, and helps ensure the Director of Mission Operations and senior leadership have timely, decision-ready information to advance the Command's mission.

General Counsel

The General Counsel serves as the Command's chief legal advisor, providing counsel to executive leadership and staff on the laws, authorities, policies, and legal risks governing the Command's statewide cybersecurity mission. The General Counsel maintains direct and independent communications to and with the Chief, advises on contracts and procurement, interagency and information-sharing agreements, cybersecurity and data-governance matters, ethics, employment, public information and confidentiality, litigation coordination, and other agency legal matters.

Chief Procurement Officer

The Chief Procurement Officer oversees the agency's procurement, contracting, and contract management activities, ensuring technology, telecommunications, and operational needs are acquired efficiently and in compliance with applicable requirements. The Chief Procurement Officer also provides leadership over procurement services, contract administration, and related programs to support the Command's mission and business operations.

Chief Financial Officer

The Chief Financial Officer directs TXCC's financial management, budget execution, financial reporting, and related business operations to ensure the agency's resources are aligned with statutory responsibilities and statewide cybersecurity priorities. The Chief Financial Officer provides executive leadership with timely financial analysis and decision support, ensures compliance with applicable fiscal laws and requirements, oversees the responsible stewardship of appropriated funds and fund balances, and drives continuous improvement in financial and administrative processes.

Chief of Human Resources

The Chief of Human Resources (HR) leads the Command's workforce strategy, employee relations, internships, performance management, compensation, and personnel policies. The Chief of HR ensures HR programs support the Command's mission, comply with applicable laws and policies, and foster a high-performing and engaged workforce.

Director of the Project and Portfolio Management Office

The Director of the Project and Portfolio Management Office (PPMO) oversees the planning, governance, prioritization, and execution of the agency's portfolio of projects and strategic initiatives. The Director ensures projects align with organizational priorities, effectively manage resources and risks, and deliver measurable outcomes that advance the Command's mission.

Director of Public Affairs

The Director of Public Affairs leads the agency's communications, media relations, public information, and stakeholder engagement efforts to ensure clear and consistent messaging. The Director manages external communications, supports executive leadership, promotes public awareness of the agency's mission, and coordinates communications during significant events and cyber incidents.

Executive Operations Manager

The Executive Operations Manager oversees and coordinates executive-level operations, ensuring leadership priorities, meetings, communications, and key initiatives are effectively organized and executed. The Executive Operations Manager facilitates coordination across divisions, tracks executive action items and deliverables, and provides operational support to help agency leadership advance strategic priorities.

Chief Strategy Officer

The Chief Strategy Officer leads the development and execution of the agency's strategic vision, ensuring priorities, initiatives, and resources are aligned with its mission and long-term goals. The Chief Strategy Officer works across the organization to drive strategic planning, measure performance, identify emerging opportunities and risks, and ensure leadership priorities translate into measurable results.

Director of Strategy and Planning

The Director of Strategy and Planning leads the development, coordination, and implementation of the agency's strategic plans, ensuring organizational priorities and initiatives align with its mission and long-term objectives. The Director works across divisions to establish goals, track performance, assess emerging needs and risks, and translate leadership priorities into actionable plans and measurable outcomes.

Director of Unified Cyber Task Force

The Director of the Unified Cyber Task Force (UCTF) leads the UCTF as TXCC's internal operating construct for integrated statewide cyber defense and reports to the Deputy Chief. The Director sets operational priorities, watch posture, force readiness, resource allocation, and cross-component execution across the Command, the SOC, CIRU, and DFL, while elevating material risks, exceptions, and resource conflicts requiring Deputy Chief attention.

Director of the Cyber Threat Intelligence Center

The Director of the CTIC reports to the Intel Chief and is responsible for leading and developing CTIC analysts producing strategic, operational, and tactical cyber threat intelligence; advancing intelligence tradecraft, quality standards, and the full threat intelligence lifecycle.

Assistant Director of Unified Cyber Task Force

The Assistant Director of UTCF serves as the principal deputy to the Director of UCTF and manages the daily operating rhythm, common operational picture, tasking, performance tracking, workforce synchronization, and continuity of UCTF operations. The Assistant Director directly coordinates and supervises the SOC, CIRU, and DFL directors, resolves routine cross-component friction, and acts for the Director when delegated.

Director of Cyber Incident Response Unit

The Director of the Cyber Incident Response Unit (CIRU) directs statewide cyber incident response operations, including state agency monitoring and Tier 1 support where assigned, incident command, advanced response, containment, threat neutralization, recovery support, and post-incident monitoring. The Director of CIRU maintains readiness, duty coverage, playbooks, surge coordination, and partner integration while coordinating with DFL on evidence and forensic requirements and with CTIC on intelligence and statewide protective action.

Director of Security Operations Center

The Director of the Security Operations Center (SOC) directs TXCC's common security operations platform and shared services environment, including statewide visibility, security information and event management (SIEM) and threat intelligence platform integration, hotline and service desk integration, detection engineering, threat hunting, exposure management, automation, operational assurance, and platform sustainment. The Director of SOC ensures common services, data, detections, and automations are secure, reliable, and usable across UCTF and the RSOCs, while maintaining the SOC as an advanced statewide capability rather than duplicating routine frontline service delivery.

Director of Digital Forensics Laboratory

The Director of the Digital Forensics Laboratory (DFL) directs evidence preservation, chain of custody, forensic acquisition and analysis, scope-of-harm and cause analysis, remediation support, and defensible transfer of forensic materials to law enforcement and other authorized recipients. The Director establishes forensic methods, quality controls, release discipline, and continuous readiness so that DFL findings support incident response and intelligence needs without compromising evidence integrity, confidentiality, or privacy.

Director of Information Sharing Analysis Organization

The Director of the Information Sharing and Analysis Organization (ISAO) provides strategic direction, governance, and accountability for Texas Cyber Command's statewide collaboration capability. The Director sets priorities, integrates the Cybersecurity Stakeholder, Cyber Practice, and Cyber Innovation Centers, manages executive engagement, and coordinates with CTIC, UCTF, CIRU, RSOCs, and Command leadership to turn validated needs and information into coordinated statewide action.

Assistant Director of Information Sharing Analysis Organization

The Assistant Director of ISAO serves as the principal deputy responsible for day-to-day execution of the ISAO mission. The Assistant Director manages staffing, performance, operating rhythm, and cross-center requirements, tracks leadership priorities through completion, and ensures strategic direction is translated into disciplined, measurable delivery, and acts for the Director when delegated.

Director of Cyber Stakeholder Center

The Director of the Cyber Stakeholder Center (CSC) leads TXCC's statewide stakeholder and executive engagement, governed information sharing, service coordination, and regional integration. The Director builds trusted relationships across government, higher education, critical infrastructure, private industry, and regional partners and ensures validated information and requirements reach the appropriate organization for action.

Director of the Cyber Practice Center

The Director of the Cyber Practice Center (CPC) leads statewide workforce development, training, certification, cyber maturity, readiness, governance, secure collaboration platforms, and adoption of effective cyber practices. The Director integrates stakeholder requirements, threat context, operational lessons, and emerging capabilities into repeatable programs that strengthen proficiency, preparedness, and measurable cybersecurity readiness across Texas.

Director of Cyber Innovation Center

The Director of the Cyber Innovation Center (CIC) leads the identification, evaluation, validation, and transition of emerging cybersecurity capabilities that address demonstrated operational needs and reduce statewide cyber risk. The Director manages the innovation portfolio and strategic partnerships with government, private industry, and academia, ensuring emerging technologies are rigorously evaluated for operational value, readiness, scalability, and return on investment for statewide cybersecurity priorities.

Management Positions/FTEs Supervised

Management Positions	FTE Supervised
Chief	3
Vice Chief	10
Deputy Chief	5
Intelligence Chief	1
Director of Mission Operations	1
General Counsel	2
Chief Procurement Officer	2
Chief Financial Officer	2
Chief of Human Resources	2
Director of the Project and Portfolio Management Office	2
Director of Public Affairs	3
Executive Operations Manager	3
Chief Strategy Officer	1
Director of Unified Cyber Task Force	3
Director of the Cyber Threat Intelligence Center	6
Assistant Director of Unified Cyber Task Force	3
Director of Cyber Incident Response Unit	10
Director of Security Operations Center	13
Director of Digital Forensics Lab	4
Director of Information Sharing Analysis Organization	1
Assistant Director of Information Sharing Analysis Organization	3
Director of Cyber Stakeholder Center	8
Director of the Cyber Practice Center	10
Director of Cyber Innovation Center	4

CERTIFICATE

Texas Cyber Command

This is to certify that the information contained in the agency Legislative Appropriations Request filed with the Legislative Budget Board (LBB) and the Office of the Governor, Budget and Policy Division, is accurate to the best of my knowledge and that the electronic submission to the LBB via the Automated Budget and Evaluation System of Texas (ABEST) and the PDF file submitted via the LBB Document Submission application are identical.

Additionally, should it become likely at any time that unexpended balances will accrue for any account, the LBB and the Office of the Governor will be notified in writing in accordance with Senate Bill 1, Article IX, Section 7.01, Eighty-ninth Legislature, Regular Session, 2025.

Chief Executive Officer

Signature

TJ White, VADM/USN (ret)
Printed Name

Chief of Texas Cyber Command
Title

August 18, 2026
Date

Chief Financial Officer

Signature

Sami Chadli
Printed Name

Chief Financial Officer
Title

August 18, 2026
Date

371 Texas Cyber Command

Appropriation Years: 2028-29

	GENERAL REVENUE FUNDS		GR DEDICATED		FEDERAL FUNDS		OTHER FUNDS		ALL FUNDS		EXCEPTIONAL ITEM FUNDS
	2026-27	2028-29	2026-27	2028-29	2026-27	2028-29	2026-27	2028-29	2026-27	2028-29	2028-29
Goal: 1. Enhance Texas' Cybersecurity Readiness											
1.1.1. Enable Transformational Capability	32,112,594	58,563,773							32,112,594	58,563,773	80,765,922
Total, Goal	**32,112,594**	**58,563,773**							**32,112,594**	**58,563,773**	**80,765,922**
Goal: 2. Boost the State of Texas Cyber Resilience											
2.1.1. Transform Cyber Ir Capabilities	168,630,768	149,685,699							168,630,768	149,685,699	142,901,714
Total, Goal	**168,630,768**	**149,685,699**							**168,630,768**	**149,685,699**	**142,901,714**
Goal: 3. Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce											
3.1.1. Transform Training Programs	1,657,106	2,819,996							1,657,106	2,819,996	4,744,600
Total, Goal	**1,657,106**	**2,819,996**							**1,657,106**	**2,819,996**	**4,744,600**
Goal: 4. Indirect Administration											
4.1.1. Central Administration	51,524,888	32,328,127							51,524,888	32,328,127	6,572,140
Total, Goal	**51,524,888**	**32,328,127**							**51,524,888**	**32,328,127**	**6,572,140**
Total, Agency	**253,925,356**	**243,397,595**							**253,925,356**	**243,397,595**	**234,984,376**
Total FTEs									**92.0**	**92.0**	**120.0**

371 Texas Cyber Command

Goal / *Objective* / STRATEGY	Exp 2025	Est 2026	Bud 2027	Req 2028	Req 2029
1 Enhance Texas' Cybersecurity Readiness					
1 *Build Out and Elevate Texas Cyber Command's "Prevent" Mission*					
1 ENABLE TRANSFORMATIONAL CAPABILITY	0	2,929,296	29,183,298	30,698,741	27,865,032
TOTAL, GOAL 1	**$0**	**$2,929,296**	**$29,183,298**	**$30,698,741**	**$27,865,032**
2 Boost the State of Texas Cyber Resilience					
1 *Respond to and Recover from Malicious Cyber Intrusions*					
1 TRANSFORM CYBER IR CAPABILITIES	0	97,105,744	71,525,024	76,030,310	73,655,389
TOTAL, GOAL 2	**$0**	**$97,105,744**	**$71,525,024**	**$76,030,310**	**$73,655,389**
3 Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce					
1 *Facilitate Education and Training of a Future Cybersecurity Workforce*					
1 TRANSFORM TRAINING PROGRAMS	0	247,461	1,409,645	1,409,608	1,410,388
TOTAL, GOAL 3	**$0**	**$247,461**	**$1,409,645**	**$1,409,608**	**$1,410,388**

371 Texas Cyber Command

Goal / *Objective* / STRATEGY	Exp 2025	Est 2026	Bud 2027	Req 2028	Req 2029
4 Indirect Administration					
1 *Central Administration*					
1 CENTRAL ADMINISTRATION	0	31,209,727	20,315,161	16,258,295	16,069,832
TOTAL, GOAL 4	**$0**	**$31,209,727**	**$20,315,161**	**$16,258,295**	**$16,069,832**
TOTAL, AGENCY STRATEGY REQUEST	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
TOTAL, AGENCY RIDER APPROPRIATIONS REQUEST*				**$0**	**$0**
GRAND TOTAL, AGENCY REQUEST	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
METHOD OF FINANCING:					
General Revenue Funds:					
1 General Revenue Fund	0	131,492,228	122,433,128	124,396,954	119,000,641
SUBTOTAL	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
TOTAL, METHOD OF FINANCING	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**

*Rider appropriations for the historical years are included in the strategy amounts.

Agency code: **371** Agency name: **Texas Cyber Command**

METHOD OF FINANCING	Exp 2025	Est 2026	Bud 2027	Req 2028	Req 2029
GENERAL REVENUE					
1 General Revenue Fund					
REGULAR APPROPRIATIONS					
TXCC Cybersecurity Base Appropriations	$0	$0	$0	$121,396,954	$116,000,641
Comments: Continuation of cybersecurity GR funding transferred from Agency 313 to Agency 371 pursuant to H.B. 150, 89th Leg., R.S. The FY 2028-29 biennial base request reflects the required 3% reduction in accordance with current LBB guidance.					
RIDER APPROPRIATION					
SB 1, 89R, CCR Art. I, DIR Rider 12	$0	$3,000,000	$0	$3,000,000	$3,000,000
Comments: Fiscal Rider 12 Paragraph 2					
TRANSFERS					
Cybersecurity appns. 29813, 39013, 39108, and 13022 to reflect biennial GR transfers from Agency 313 to Agency 371.	$0	$222,352,463	$28,572,893	$0	$0

Agency code: **371** Agency name: **Texas Cyber Command**

METHOD OF FINANCING	Exp 2025	Est 2026	Bud 2027	Req 2028	Req 2029
GENERAL REVENUE					
Comments: The total biennial amount transferred is $250,925,356, broken down as follows: $10,000,000 - HB 500, 89R, Sec. 1.08, DIR Existing RSOCs - Biennial amount $48,243,334 - HB 500, 89R, Sec. 10.13, DIR Cybersecurity Expansion - Biennial amount $135,536,236 - Article IX, Contingency for HB 150 or SB 2176, Texas Cyber Command - Biennial amount $28,572,893 - SB 1, 89R, CCR Art. I, DIR Rider 12, C.1.2 Security Services cyber portion - FY 2026 amount $28,572,893 - SB 1, 89R, CCR Art. I, DIR Rider 12, C.1.2 Security Services cyber portion - FY 2027 amount					
UNEXPENDED BALANCES AUTHORITY					
Anticipated FY 2026 UB to FY 2027, based on actual expenditures and projections provided by DIR.	$0	$(93,860,235)	$93,860,235	$0	$0
Comments: Anticipated FY 2026 transferred-fund UB carried forward to FY 2027, based on actual expenditures and projections provided by DIR.					
TOTAL, General Revenue Fund	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
TOTAL, ALL GENERAL REVENUE	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**

Agency code: **371** Agency name: **Texas Cyber Command**

METHOD OF FINANCING	Exp 2025	Est 2026	Bud 2027	Req 2028	Req 2029
GRAND TOTAL	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
FULL-TIME-EQUIVALENT POSITIONS					
REGULAR APPROPRIATIONS					
2028–29 Baseline Request – Continuation of TXCC FTEs **Comments:** Continuation of FTE authority transferred to Texas Cyber Command pursuant to H.B. 150, 89th Leg., R.S., Sec. 50(d) and Sec. 50(e). Includes 38.0 FTEs transferred pursuant to the Article IX contingency and 46.0 legacy DIR staff transferred to TXCC.	0.0	0.0	0.0	92.0	92.0
TRANSFERS					
Article IX, Contingency for HB 150 or SB 2176 - Texas Cyber Command **Comments:** H.B. 150, 89th Leg., R.S., Sec. 50(d) and Sec. 50(e)	0.0	38.0	46.0	0.0	0.0
Regular Appropriations from MOF Table (2026-27 GAA) **Comments:** Legacy DIR Staff Absorbed - H.B. 150, 89th Leg., R.S., Sec. 50(d)	0.0	23.0	46.0	0.0	0.0
TOTAL, ADJUSTED FTES	**0.0**	**61.0**	**92.0**	**92.0**	**92.0**
NUMBER OF 100% FEDERALLY FUNDED FTEs	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

371 Texas Cyber Command

OBJECT OF EXPENSE	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
1001 SALARIES AND WAGES	$0	$4,373,742	$13,624,476	$13,624,476	$13,624,476
1002 OTHER PERSONNEL COSTS	$0	$40,875	$266,427	$271,607	$277,227
2001 PROFESSIONAL FEES AND SERVICES	$0	$64,324,756	$38,778,298	$36,809,840	$35,618,668
2003 CONSUMABLE SUPPLIES	$0	$12,643	$20,450	$20,475	$20,500
2004 UTILITIES	$0	$29,810	$21,000	$21,000	$21,000
2005 TRAVEL	$0	$58,718	$218,614	$233,000	$242,500
2007 RENT - MACHINE AND OTHER	$0	$2,800,000	$2,800,000	$2,800,000	$0
2009 OTHER OPERATING EXPENSE	$0	$59,817,232	$60,203,863	$70,616,556	$69,196,270
5000 CAPITAL EXPENDITURES	$0	$34,452	$6,500,000	$0	$0
OOE Total (Excluding Riders)	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
OOE Total (Riders)					
Grand Total	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**

371 Texas Cyber Command

Goal/ *Objective* / **Outcome**	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
2 Boost the State of Texas Cyber Resilience					
1 Respond to and Recover from Malicious Cyber Intrusions					
1 Change in Cyber Incidents of the Same or Similar Nature	0.00%	0.00%	0.00%	5.00%	3.00%
KEY 2 Reduction in Average Time from Compromise to Detection and Mitigation	0.00	0.00	0.00	1,080.00	720.00
KEY 3 Percent Change in Agencies' Security Maturity Over Repeat Assessments	0.00%	0.00%	3.00%	0.00%	0.00%

Agency code: **371** Agency name: **Texas Cyber Command**

Priority	Item	2028 GR and GR/GR Dedicated	2028 All Funds	2028 FTEs	2029 GR and GR Dedicated	2029 All Funds	2029 FTEs	Biennium GR and GR Dedicated	Biennium All Funds
1	Cost Recovery	$27,665,400	$27,665,400		$26,752,644	$26,752,644		$54,418,044	$54,418,044
2	TXCC Statutory Staffing	$14,568,166	$14,568,166	120.0	$14,568,166	$14,568,166	120.0	$29,136,332	$29,136,332
3	AI and Quantum Risk	$18,000,000	$18,000,000		$23,500,000	$23,500,000		$41,500,000	$41,500,000
4	ISAO Governance Modernization	$6,215,000	$6,215,000		$6,215,000	$6,215,000		$12,430,000	$12,430,000
5	CTIC Threat Warning	$9,150,000	$9,150,000		$9,150,000	$9,150,000		$18,300,000	$18,300,000
6	Incident Intake and Recovery	$6,800,000	$6,800,000		$6,800,000	$6,800,000		$13,600,000	$13,600,000
7	Shared Cyber Protection	$39,800,000	$39,800,000		$25,800,000	$25,800,000		$65,600,000	$65,600,000
Total, Exceptional Items Request		**$122,198,566**	**$122,198,566**	**120.0**	**$112,785,810**	**$112,785,810**	**120.0**	**$234,984,376**	**$234,984,376**
Method of Financing									
	General Revenue	$122,198,566	$122,198,566		$112,785,810	$112,785,810		$234,984,376	$234,984,376
	General Revenue - Dedicated								
	Federal Funds								
	Other Funds								
		$122,198,566	**$122,198,566**		**$112,785,810**	**$112,785,810**		**$234,984,376**	**$234,984,376**
Full Time Equivalent Positions				**120.0**			**120.0**		
Number of 100% Federally Funded FTEs				**0.0**			**0.0**		

Agency code: **371** Agency name: **Texas Cyber Command**

Goal/*Objective*/STRATEGY	Base 2028	Base 2029	Exceptional 2028	Exceptional 2029	Total Request 2028	Total Request 2029
1 Enhance Texas' Cybersecurity Readiness						
1 *Build Out and Elevate Texas Cyber Command's "Prevent" Mission*						
1 ENABLE TRANSFORMATIONAL CAPABILITY	$30,698,741	$27,865,032	$37,632,961	$43,132,961	$68,331,702	$70,997,993
TOTAL, GOAL 1	**$30,698,741**	**$27,865,032**	**$37,632,961**	**$43,132,961**	**$68,331,702**	**$70,997,993**
2 Boost the State of Texas Cyber Resilience						
1 *Respond to and Recover from Malicious Cyber Intrusions*						
1 TRANSFORM CYBER IR CAPABILITIES	76,030,310	73,655,389	78,907,235	63,994,479	154,937,545	137,649,868
TOTAL, GOAL 2	**$76,030,310**	**$73,655,389**	**$78,907,235**	**$63,994,479**	**$154,937,545**	**$137,649,868**
3 Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce						
1 *Facilitate Education and Training of a Future Cybersecurity Workfor*						
1 TRANSFORM TRAINING PROGRAMS	1,409,608	1,410,388	2,372,300	2,372,300	3,781,908	3,782,688
TOTAL, GOAL 3	**$1,409,608**	**$1,410,388**	**$2,372,300**	**$2,372,300**	**$3,781,908**	**$3,782,688**

Agency code: **371** Agency name: **Texas Cyber Command**

Goal/*Objective*/**STRATEGY**	**Base 2028**	**Base 2029**	**Exceptional 2028**	**Exceptional 2029**	**Total Request 2028**	**Total Request 2029**
4 Indirect Administration						
1 *Central Administration*						
1 CENTRAL ADMINISTRATION	$16,258,295	$16,069,832	$3,286,070	$3,286,070	$19,544,365	$19,355,902
TOTAL, GOAL 4	**$16,258,295**	**$16,069,832**	**$3,286,070**	**$3,286,070**	**$19,544,365**	**$19,355,902**
TOTAL, AGENCY STRATEGY REQUEST	**$124,396,954**	**$119,000,641**	**$122,198,566**	**$112,785,810**	**$246,595,520**	**$231,786,451**
TOTAL, AGENCY RIDER APPROPRIATIONS REQUEST						
GRAND TOTAL, AGENCY REQUEST	**$124,396,954**	**$119,000,641**	**$122,198,566**	**$112,785,810**	**$246,595,520**	**$231,786,451**

Agency code: **371** Agency name: **Texas Cyber Command**

Goal/*Objective*/**STRATEGY**	**Base 2028**	**Base 2029**	**Exceptional 2028**	**Exceptional 2029**	**Total Request 2028**	**Total Request 2029**
General Revenue Funds:						
1 General Revenue Fund	$124,396,954	$119,000,641	$122,198,566	$112,785,810	$246,595,520	$231,786,451
	$124,396,954	**$119,000,641**	**$122,198,566**	**$112,785,810**	**$246,595,520**	**$231,786,451**
TOTAL, METHOD OF FINANCING	**$124,396,954**	**$119,000,641**	**$122,198,566**	**$112,785,810**	**$246,595,520**	**$231,786,451**
FULL TIME EQUIVALENT POSITIONS	**92.0**	**92.0**	**120.0**	**120.0**	**212.0**	**212.0**

Agency code: **371** Agency name: **Texas Cyber Command**

Goal/ *Objective* / **Outcome**

		BL 2028	BL 2029	Excp 2028	Excp 2029	Total Request 2028	Total Request 2029
2	Boost the State of Texas Cyber Resilience						
1	*Respond to and Recover from Malicious Cyber Intrusions*						
	1 Change in Cyber Incidents of the Same or Similar Nature	5.00%	3.00%			5.00%	3.00%
KEY	**2 Reduction in Average Time from Compromise to Detection and Mitigation**	1,080.00	720.00			1,080.00	720.00
KEY	**3 Percent Change in Agencies' Security Maturity Over Repeat Assessments**	0.00%	0.00%			0.00%	0.00%

371 Texas Cyber Command

GOAL: 1 Enhance Texas' Cybersecurity Readiness

OBJECTIVE: 1 Build Out and Elevate Texas Cyber Command's "Prevent" Mission — Service Categories:

STRATEGY: 1 Enable CTIC, ISAO, and DFL with Transformational Capabilities — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
Output Measures:						
1	Threat Intelligence Alerts, Advisories, and Recommendations Issued	0.00	0.00	45.00	45.00	45.00
Efficiency Measures:						
KEY 1	Time to Disseminate Threat Intelligence	0.00	0.00	504.00	336.00	336.00
Objects of Expense:						
1001	SALARIES AND WAGES	$0	$823,941	$4,648,932	$4,648,932	$4,648,932
1002	OTHER PERSONNEL COSTS	$0	$15,754	$74,374	$75,154	$76,054
2001	PROFESSIONAL FEES AND SERVICES	$0	$2,020,392	$8,056,233	$6,000,000	$5,000,000
2003	CONSUMABLE SUPPLIES	$0	$0	$2,000	$2,000	$2,000
2004	UTILITIES	$0	$0	$4,200	$4,200	$4,200
2005	TRAVEL	$0	$27,175	$120,000	$120,000	$120,000
2009	OTHER OPERATING EXPENSE	$0	$42,034	$16,277,559	$19,848,455	$18,013,846
5000	CAPITAL EXPENDITURES	$0	$0	$0	$0	$0
TOTAL, OBJECT OF EXPENSE		**$0**	**$2,929,296**	**$29,183,298**	**$30,698,741**	**$27,865,032**
Method of Financing:						
1	General Revenue Fund	$0	$2,929,296	$29,183,298	$30,698,741	$27,865,032

371 Texas Cyber Command

GOAL: 1 Enhance Texas' Cybersecurity Readiness

OBJECTIVE: 1 Build Out and Elevate Texas Cyber Command's "Prevent" Mission — Service Categories:

STRATEGY: 1 Enable CTIC, ISAO, and DFL with Transformational Capabilities — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
SUBTOTAL, MOF (GENERAL REVENUE FUNDS)		**$0**	**$2,929,296**	**$29,183,298**	**$30,698,741**	**$27,865,032**
TOTAL, METHOD OF FINANCE (INCLUDING RIDERS)					**$30,698,741**	**$27,865,032**
TOTAL, METHOD OF FINANCE (EXCLUDING RIDERS)		**$0**	**$2,929,296**	**$29,183,298**	**$30,698,741**	**$27,865,032**
FULL TIME EQUIVALENT POSITIONS:		**0.0**	**15.0**	**31.0**	**31.0**	**31.0**

STRATEGY DESCRIPTION AND JUSTIFICATION:

Protect state government and critical infrastructure information and operational networks and assets by delivering state-of-the-art cybersecurity services, expanding operational capacity, and collaborating with appropriate state, local, and federal entities.

EXTERNAL/INTERNAL FACTORS IMPACTING STRATEGY:

371 Texas Cyber Command

GOAL: 1 Enhance Texas' Cybersecurity Readiness

OBJECTIVE: 1 Build Out and Elevate Texas Cyber Command's "Prevent" Mission — Service Categories:

STRATEGY: 1 Enable CTIC, ISAO, and DFL with Transformational Capabilities — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029

Achieving this goal depends on several operational factors. Recruiting and retaining qualified cybersecurity professionals remains a challenge due to statewide workforce shortages and competition with the private sector. Progress also relies on consistent participation from partner agencies and critical infrastructure entities, whose cybersecurity maturity and resource levels vary significantly. Legacy systems and aging technology across the state may limit the deployment of modern security controls without additional modernization funding. Finally, the rapidly evolving threat and technology landscape, in particular the emergence of AI in cyber offense and cyber defense, requires ongoing investment in tools, training, and statewide coordination to maintain readiness.

EXPLANATION OF BIENNIAL CHANGE (includes Rider amounts):

STRATEGY BIENNIAL TOTAL - ALL FUNDS		BIENNIAL	EXPLANATION OF BIENNIAL CHANGE	
Base Spending (Est 2026 + Bud 2027)	Baseline Request (BL 2028 + BL 2029)	CHANGE	$ Amount	Explanation(s) of Amount (must specify MOFs and FTEs)
$32,112,594	$58,563,773	$26,451,179	$26,451,179	Budget Structure and Cost Realignment – Amount reflects cost realignment to agency's new budget structure and updated spending projections for FTEs and planned procurements and renewals.
			$26,451,179	**Total of Explanation of Biennial Change**

371 Texas Cyber Command

GOAL: 2 Boost the State of Texas Cyber Resilience

OBJECTIVE: 1 Respond to and Recover from Malicious Cyber Intrusions — Service Categories:

STRATEGY: 1 Transform Cyber Incident Response Capabilities Transferred — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
Output Measures:						
KEY	1 Entities Receiving Continuous Diagnostics and Mitigation Services	0.00	0.00	290.00	325.00	345.00
	2 Coordinated Cyber Defense and Tabletop Exercises Conducted	0.00	0.00	4.00	6.00	8.00
KEY	3 Entities with Active RSOC Service Agreements	0.00	0.00	700.00	720.00	745.00
	4 Number of Students Participating in RSOC Programs and Activities	0.00	0.00	110.00	115.00	120.00
KEY	5 Number of Completed State Security Assessments	0.00	0.00	40.00	40.00	40.00
KEY	6 Number of Completed Penetration Tests	0.00	0.00	50.00	50.00	50.00
Efficiency Measures:						
	1 Cost Per Completed Penetration Test Delivered to Eligible Entities	0.00	0.00	21,768.00	20,000.00	20,000.00
Objects of Expense:						
1001	SALARIES AND WAGES	$0	$1,440,502	$3,859,423	$3,859,423	$3,859,423
1002	OTHER PERSONNEL COSTS	$0	$8,877	$72,011	$74,191	$75,851
2001	PROFESSIONAL FEES AND SERVICES	$0	$56,117,663	$29,206,373	$29,436,320	$29,445,388
2003	CONSUMABLE SUPPLIES	$0	$8,544	$6,050	$6,050	$6,050
2005	TRAVEL	$0	$5,900	$2,500	$2,500	$2,500

371 Texas Cyber Command

GOAL: 2 Boost the State of Texas Cyber Resilience

OBJECTIVE: 1 Respond to and Recover from Malicious Cyber Intrusions — Service Categories:

STRATEGY: 1 Transform Cyber Incident Response Capabilities Transferred — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
2007	RENT - MACHINE AND OTHER	$0	$2,800,000	$2,800,000	$2,800,000	$0
2009	OTHER OPERATING EXPENSE	$0	$36,724,258	$35,578,667	$39,851,826	$40,266,177
5000	CAPITAL EXPENDITURES	$0	$0	$0	$0	$0
TOTAL, OBJECT OF EXPENSE		**$0**	**$97,105,744**	**$71,525,024**	**$76,030,310**	**$73,655,389**
Method of Financing:						
1	General Revenue Fund	$0	$97,105,744	$71,525,024	$76,030,310	$73,655,389
SUBTOTAL, MOF (GENERAL REVENUE FUNDS)		**$0**	**$97,105,744**	**$71,525,024**	**$76,030,310**	**$73,655,389**
TOTAL, METHOD OF FINANCE (INCLUDING RIDERS)					**$76,030,310**	**$73,655,389**
TOTAL, METHOD OF FINANCE (EXCLUDING RIDERS)		**$0**	**$97,105,744**	**$71,525,024**	**$76,030,310**	**$73,655,389**
FULL TIME EQUIVALENT POSITIONS:		**0.0**	**19.0**	**28.0**	**28.0**	**28.0**

STRATEGY DESCRIPTION AND JUSTIFICATION:

Enhance Texas's ability to effectively and efficiently respond to and recover from disruptive and destructive cyber intrusions.

371 Texas Cyber Command

GOAL: 2 Boost the State of Texas Cyber Resilience

OBJECTIVE: 1 Respond to and Recover from Malicious Cyber Intrusions — Service Categories:

STRATEGY: 1 Transform Cyber Incident Response Capabilities Transferred — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029

EXTERNAL/INTERNAL FACTORS IMPACTING STRATEGY:

Efforts to strengthen statewide cyber resilience are influenced by the varying levels of business continuity, disaster recovery, and incident response preparedness across governmental and critical infrastructure entities. Many organizations operate legacy systems or fragmented environments that complicate the implementation of modern backup, redundancy, and recovery capabilities. Resilience activities also require trained personnel beyond cybersecurity teams, including operational and IT staff who can execute continuity and recovery procedures. Sustained funding and coordinated planning
across agencies, local governments, and external partners are essential to support long-term resilience improvements.

EXPLANATION OF BIENNIAL CHANGE (includes Rider amounts):

STRATEGY BIENNIAL TOTAL - ALL FUNDS		BIENNIAL	EXPLANATION OF BIENNIAL CHANGE	
Base Spending (Est 2026 + Bud 2027)	Baseline Request (BL 2028 + BL 2029)	CHANGE	$ Amount	Explanation(s) of Amount (must specify MOFs and FTEs)
$168,630,768	$149,685,699	$(18,945,069)	$(18,945,069)	Budget Structure and Cost Realignment – Amount reflects cost realignment to agency's new budget structure and updated spending projections for FTEs and planned procurements and renewals.
			$(18,945,069)	**Total of Explanation of Biennial Change**

371 Texas Cyber Command

GOAL: 3 Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce

OBJECTIVE: 1 Facilitate Education and Training of a Future Cybersecurity Workforce — Service Categories:

STRATEGY: 1 Transform Training and Education Programs Transferred from DIR to TXCC — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
Output Measures:						
KEY 1	Percentage of Entities Participating in Cybersecurity Training	0.00%	0.00 %	65.00 %	65.00 %	65.00 %
Objects of Expense:						
1001	SALARIES AND WAGES	$0	$239,277	$1,379,909	$1,379,909	$1,379,909
1002	OTHER PERSONNEL COSTS	$0	$8,184	$25,219	$25,639	$26,419
2009	OTHER OPERATING EXPENSE	$0	$0	$4,517	$4,060	$4,060
TOTAL, OBJECT OF EXPENSE		**$0**	**$247,461**	**$1,409,645**	**$1,409,608**	**$1,410,388**
Method of Financing:						
1	General Revenue Fund	$0	$247,461	$1,409,645	$1,409,608	$1,410,388
SUBTOTAL, MOF (GENERAL REVENUE FUNDS)		**$0**	**$247,461**	**$1,409,645**	**$1,409,608**	**$1,410,388**
TOTAL, METHOD OF FINANCE (INCLUDING RIDERS)					**$1,409,608**	**$1,410,388**
TOTAL, METHOD OF FINANCE (EXCLUDING RIDERS)		**$0**	**$247,461**	**$1,409,645**	**$1,409,608**	**$1,410,388**
FULL TIME EQUIVALENT POSITIONS:		**0.0**	**5.0**	**10.0**	**10.0**	**10.0**

371 Texas Cyber Command

GOAL:	3	Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce			
OBJECTIVE:	1	Facilitate Education and Training of a Future Cybersecurity Workforce	Service Categories:		
STRATEGY:	1	Transform Training and Education Programs Transferred from DIR to TXCC	Service: 35	Income: A.2	Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029

STRATEGY DESCRIPTION AND JUSTIFICATION:

Ensure the state of Texas is growing the cybersecurity workforce it will need to protect its future in cyberspace against current and future cyber threats.

EXTERNAL/INTERNAL FACTORS IMPACTING STRATEGY:

Achieving this goal depends on several factors that influence the development of a highly skilled cybersecurity workforce in Texas. The agency’s ability to deliver high-quality training programs is shaped by access to up-to-date training environments and the resources required to maintain relevant curricula as threats and technologies evolve. Workforce development also relies on the broader ecosystem of universities, community colleges, technical institutions, and industry partners, whose capacity and alignment with statewide needs vary across regions. Public sector competitiveness remains a challenge as state agencies often face salary and hiring constraints that limit their ability to attract and retain cybersecurity professionals. Sustained funding and strong coordination with education partners, industry, and other state agencies are essential to expand training opportunities and strengthen the statewide cybersecurity talent pipeline.

371 Texas Cyber Command

GOAL: 3 Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce

OBJECTIVE: 1 Facilitate Education and Training of a Future Cybersecurity Workforce — Service Categories:

STRATEGY: 1 Transform Training and Education Programs Transferred from DIR to TXCC — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029

EXPLANATION OF BIENNIAL CHANGE (includes Rider amounts):

STRATEGY BIENNIAL TOTAL - ALL FUNDS		BIENNIAL	EXPLANATION OF BIENNIAL CHANGE	
Base Spending (Est 2026 + Bud 2027)	Baseline Request (BL 2028 + BL 2029)	CHANGE	$ Amount	Explanation(s) of Amount (must specify MOFs and FTEs)
$1,657,106	$2,819,996	$1,162,890	$1,162,890	Budget Structure and Cost Realignment – Amount reflects cost realignment to agency's new budget structure and updated spending projections for FTEs and planned procurements and renewals.
			$1,162,890	**Total of Explanation of Biennial Change**

371 Texas Cyber Command

GOAL: 4 Indirect Administration

OBJECTIVE: 1 Central Administration — Service Categories:

STRATEGY: 1 Central Administration — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
Objects of Expense:						
1001	SALARIES AND WAGES	$0	$1,870,022	$3,736,212	$3,736,212	$3,736,212
1002	OTHER PERSONNEL COSTS	$0	$8,060	$94,823	$96,623	$98,903
2001	PROFESSIONAL FEES AND SERVICES	$0	$6,186,701	$1,515,692	$1,373,520	$1,173,280
2003	CONSUMABLE SUPPLIES	$0	$4,099	$12,400	$12,425	$12,450
2004	UTILITIES	$0	$29,810	$16,800	$16,800	$16,800
2005	TRAVEL	$0	$25,643	$96,114	$110,500	$120,000
2009	OTHER OPERATING EXPENSE	$0	$23,050,940	$8,343,120	$10,912,215	$10,912,187
5000	CAPITAL EXPENDITURES	$0	$34,452	$6,500,000	$0	$0
TOTAL, OBJECT OF EXPENSE		**$0**	**$31,209,727**	**$20,315,161**	**$16,258,295**	**$16,069,832**
Method of Financing:						
1	General Revenue Fund	$0	$31,209,727	$20,315,161	$16,258,295	$16,069,832
SUBTOTAL, MOF (GENERAL REVENUE FUNDS)		**$0**	**$31,209,727**	**$20,315,161**	**$16,258,295**	**$16,069,832**

371 Texas Cyber Command

GOAL: 4 Indirect Administration
OBJECTIVE: 1 Central Administration — Service Categories:
STRATEGY: 1 Central Administration — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029
TOTAL, METHOD OF FINANCE (INCLUDING RIDERS)					**$16,258,295**	**$16,069,832**
TOTAL, METHOD OF FINANCE (EXCLUDING RIDERS)		**$0**	**$31,209,727**	**$20,315,161**	**$16,258,295**	**$16,069,832**
FULL TIME EQUIVALENT POSITIONS:		**0.0**	**22.0**	**23.0**	**23.0**	**23.0**

STRATEGY DESCRIPTION AND JUSTIFICATION:

Indirect Administration provides executive leadership, financial management, legal support, procurement support, human resources coordination, policy coordination, records support, reporting support, and other administrative functions necessary to sustain agency operations and statutory responsibilities.

EXTERNAL/INTERNAL FACTORS IMPACTING STRATEGY:

The agency will ensure that each person classified as a contract manager is trained and certified in contract management.

371 Texas Cyber Command

GOAL: 4 Indirect Administration

OBJECTIVE: 1 Central Administration — Service Categories:

STRATEGY: 1 Central Administration — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Exp 2025	Est 2026	Bud 2027	BL 2028	BL 2029

EXPLANATION OF BIENNIAL CHANGE (includes Rider amounts):

STRATEGY BIENNIAL TOTAL - ALL FUNDS		BIENNIAL	EXPLANATION OF BIENNIAL CHANGE	
Base Spending (Est 2026 + Bud 2027)	Baseline Request (BL 2028 + BL 2029)	CHANGE	$ Amount	Explanation(s) of Amount (must specify MOFs and FTEs)
$51,524,888	$32,328,127	$(19,196,761)	$(19,196,761)	Budget Structure and Contract Realignment – Reflects cost realignment to TXCC’s budget structure and updated contract spending projections for planned procurements and renewals.
			$0	Budget Structure and Cost Realignment – Amount reflects cost realignment to agency's new budget structure and updated spending projections for FTEs and planned procurements and renewals.
			$(19,196,761)	**Total of Explanation of Biennial Change**

SUMMARY TOTALS:

OBJECTS OF EXPENSE:	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
METHODS OF FINANCE (INCLUDING RIDERS):				**$124,396,954**	**$119,000,641**
METHODS OF FINANCE (EXCLUDING RIDERS):	**$0**	**$131,492,228**	**$122,433,128**	**$124,396,954**	**$119,000,641**
FULL TIME EQUIVALENT POSITIONS:	**0.0**	**61.0**	**92.0**	**92.0**	**92.0**

Agency Code:	Agency Name:	Prepared By:	Date:	Request Level:
371	Texas Cyber Command	Sami Chadli	August 18, 2026	N/A

Current Rider Number	Page Number in 2026-27 GAA	Proposed Rider Language

No rider revisions and additions requested.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029
	Item Name: Sustain Cybersecurity Services Transferred From DIR and Cost-Recovery Funding		
	Item Priority: 1		
	IT Component: No		
	Anticipated Out-year Costs: No		
	Involve Contracts > $50,000: No		
	Includes Funding for the Following Strategy or Strategies: 02-01-01 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
2009	OTHER OPERATING EXPENSE	27,665,400	26,752,644
	TOTAL, OBJECT OF EXPENSE	**$27,665,400**	**$26,752,644**
METHOD OF FINANCING:			
1	General Revenue Fund	27,665,400	26,752,644
	TOTAL, METHOD OF FINANCING	**$27,665,400**	**$26,752,644**

DESCRIPTION / JUSTIFICATION:

HB 150 transferred specified cybersecurity and network security functions, personnel, contracts, property, records, and appropriated funds from the Department of Information Resources (DIR) to the Texas Cyber Command (TXCC).

Government Code Chapter 2059 assigns the provision of network security services to TXCC.

The transferred DIR strategy B.2.1--Shared Technology Services (also in Rider 9) was supported by cost recovery incorporated in the amounts below.

This item sustains existing network security services. It does not establish or expand a program.

Sections 2059.151 and 152 mandate cost recovery for these services in perpetuity from DIR to TXCC.

Chapter 2063 assigns TXCC statewide cybersecurity responsibilities that include minimum standards and training; threat intelligence and information sharing; incident support and reporting; and cloud risk and authorization management.

The transferred DIR strategies C.1.1, Security Policy and Awareness, and C.1.2, Security Services, were supported by GR and cost recovery. FY 26-27 cost-recovery components totalled $54,418,044, including $34,094,880 from Fund 6010, $17,176,986 from Fund 6011, and $3,146,178 from Fund 6012.

TXCC requests $27,665,400 in FY 28 and $26,752,644 in FY 29 in GR to replace this historical funding source. The request sustains existing security monitoring and threat

detection, multifactor authentication, penetration testing, Texas Risk and Authorization Management Program (TX-RAMP) assessments, incident reporting and response, cybersecurity awareness and training, and shared cybersecurity services. It does not establish or expand a program.

Although Section 2063.005 permits cost recovery for services to covered entities when reasonable and practical, that authority does not provide a sustainable funding base for statewide functions and state agency services. GR aligns ongoing funding with the responsibilities transferred to TXCC and helps prevent a service gap.

EXTERNAL/INTERNAL FACTORS:

External factors include vendor pricing and renewals, subscription and licensing models, service demand, participating-entity enrollment, procurement lead times, and changes in the threat environment.

Internal factors include the transition of DIR contracts and service records, governance of eligibility, service levels, cost allocation, performance monitoring, and coordination across TXCC's reporting, response, training, cloud-assurance, and network-security responsibilities.

Without this item, the loss of historical cost-recovery support would require reductions, reprioritization, or discontinuation of existing services. These reductions would occur as TXCC assumes the transferred responsibilities, increasing the risk of uneven coverage and reduced service levels.

Full funding preserves continuity of services. Partial funding would require documented service-level reductions based on statutory obligations, existing contract commitments, entity coverage, and operational risk.

PCLS TRACKING KEY:

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION		Excp 2028	Excp 2029
	Item Name:	Workforce Capacity to Execute Statewide Cybersecurity Mandates		
	Item Priority:	2		
	IT Component:	No		
	Anticipated Out-year Costs:	Yes		
	Involve Contracts > $50,000:	No		
	Includes Funding for the Following Strategy or Strategies:	01-01-01 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
		02-01-01 Transform Cyber Incident Response Capabilities Transferred		
		03-01-01 Transform Training and Education Programs Transferred from DIR to TXCC		
		04-01-01 Central Administration		
OBJECTS OF EXPENSE:				
1001	SALARIES AND WAGES		14,352,875	14,352,875
1002	OTHER PERSONNEL COSTS		215,291	215,291
	TOTAL, OBJECT OF EXPENSE		**$14,568,166**	**$14,568,166**
METHOD OF FINANCING:				
1	General Revenue Fund		14,568,166	14,568,166
	TOTAL, METHOD OF FINANCING		**$14,568,166**	**$14,568,166**
FULL-TIME EQUIVALENT POSITIONS (FTE):			120.00	120.00

DESCRIPTION / JUSTIFICATION:

Texas Government Code Chapters 2059 and 2063 establishe the Texas Cyber Command (TXCC) as the state's central authority for coordinating and executing the statewide cybersecurity mission. The statutes assigns TXCC continuing responsibilities for prevention and response, threat intelligence and warning, incident reporting and intake, digital forensics, information sharing, partnerships, minimum cybersecurity standards, workforce development, statewide planning, risk and authorization management, statewide reporting, regional security operations, network security services, and volunteer incident response.

Chapter 2063 also directs TXCC to employ the coordinating, planning, and other personnel necessary to carry out these responsibilities.

The baseline request currently supports 84 FTEs. This Exceptional Item requests 120 additional FTEs and $14,568,166 in each fiscal year, resulting in a total requested complement of 204 FTEs if fully funded.

The additional positions will expand threat analysis and warning; 24-hour intake, coordination, response, and recovery; digital evidence and forensic support; security operations; information sharing; standards, training, readiness, and assurance; partnerships; and the legal, financial, procurement, human resources, technology, communications, project management, and administrative functions required for accountable execution.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

This request is to match TXCC workforce capacity with its legislatively assigned duties, not discretionary organizational growth. It separates personnel cost from technology and service investment.

EXTERNAL/INTERNAL FACTORS:

TXCC is transitioning from initial establishment to sustained execution of the statewide cybersecurity mission directed by Government Code Chapter 2063. Initial staffing established foundational capabilities, but additional personnel are needed to perform assigned duties at the scale and continuity necessary to serve Texas.

External factors include persistent and evolving cyber threats, incident volume and severity, 24-hour operational requirements, statutory responsibilities, requests from eligible entities, and coordination with partners.

Internal factors include the need for trained state personnel to analyze threats, make operational decisions, preserve evidence, respond to incidents, assess readiness, oversee performance, and maintain fiscal and legal controls.

Without additional FTE authority, TXCC would be required to prioritize among simultaneously assigned functions, reducing statewide coverage, analytic and response capacity, information sharing, readiness assistance, and oversight.

Hiring will be phased based on mission priorities, supervisory capacity, security requirements, and available appropriations.

PCLS TRACKING KEY:

DESCRIPTION OF ANTICIPATED OUT-YEAR COSTS :

Anticipated out-year costs are the continuing salaries and related personnel costs for the requested positions, subject to enacted appropriations and statewide compensation and benefit requirements.

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$14,568,166	$14,568,166	$14,568,166
OUT-YEAR GR ONLY COSTS FOR ITEM:			
1 General Revenue Fund	$14,568,166	$14,568,166	$14,568,166
TOTAL OUT-YEAR GR ONLY:	$14,568,166	$14,568,166	$14,568,166

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029
	Item Name: Securing AI and Preparing Texas for Quantum Risk		
	Item Priority: 3		
	IT Component: Yes		
	Anticipated Out-year Costs: Yes		
	Involve Contracts > $50,000: Yes		
	Includes Funding for the Following Strategy or Strategies: 01-01-01 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	18,000,000	23,500,000
	TOTAL, OBJECT OF EXPENSE	**$18,000,000**	**$23,500,000**
METHOD OF FINANCING:			
1	General Revenue Fund	18,000,000	23,500,000
	TOTAL, METHOD OF FINANCING	**$18,000,000**	**$23,500,000**

DESCRIPTION / JUSTIFICATION:

Texas must prepare now for two technology shifts that could materially change the State's cybersecurity risk: artificial intelligence and the emergence of quantum computing, which could render much of today's data encryption and identity-management schemes obsolete.

This Exceptional Item establishes a governed statewide capability to discover, assess, test, secure, and responsibly deploy these technologies. Funding will create a statewide cryptographic inventory and transition program that includes discovery, cryptographic bills of materials, risk sequencing, readiness assessments, standards, pilots, and training.

The request also establishes an AI security and assurance program covering asset discovery, architecture review, model and artifact scanning, red-team testing, prompt and agent-abuse testing, data-leakage controls, runtime monitoring, and reusable standards. It also provides approved compute, model access, and implementation capacity for AI-assisted cyber defense under these controls.

The $41,500,000 FY 2028-29 request includes $25,000,000 for approved command AI model access, compute, automation, and engineering; $10,000,000 for statewide AI system security and assurance; and $6,500,000 for cryptographic discovery and post-quantum readiness.

The request excludes general AI application development, wholesale cryptographic replacement, named providers, and any representation that a specific capacity level or procurement has already been approved.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

EXTERNAL/INTERNAL FACTORS:

External factors include standards maturity, vendor cryptographic roadmaps, changes in models and agents, provider terms, export and data-location constraints, and uncertain consumption.

Internal factors include complete inventories, risk tiering, approved use cases, identity and access controls, logging, evidence retention, human approval, model and tool testing, data handling, consumption limits, architecture acceptance, portability, and auditable migration and production decisions.

The three workstreams have separate procurement, security, release, and acceptance gates.

The documented planning continuation is $17,000,000 annually for FY 2030 through FY 2032.

PCLS TRACKING KEY:

PCLS_90R_371_1971890

DESCRIPTION OF IT COMPONENT INCLUDED IN EXCEPTIONAL ITEM:

Cryptographic discovery and transition planning; AI system inventory and assurance; model and agent testing; approved model access and compute; automation and engineering; identity, logging, evidence, human approval, data protection, monitoring, and consumption controls.

IS THIS IT COMPONENT RELATED TO A NEW OR CURRENT PROJECT?

NEW

STATUS:

Planning and pre-procurement.

OUTCOMES:

Current cryptographic and material-AI inventories; risk-tiered transition plans; tested migration patterns; documented AI assurance decisions; approved defensive workflows; and controlled, auditable use of model and compute capacity.

OUTPUTS:

Cryptographic and AI inventories; transition roadmaps; reference patterns; assessment and test reports; authorization and exception records; approved model and agent configurations; logging and evidence records; consumption dashboards; training; and quarterly risk, cost, and readiness reporting.

TYPE OF PROJECT

Cyber Security

ALTERNATIVE ANALYSIS

The $6,500,000 cryptographic-readiness and $10,000,000 AI-assurance workstreams are independently executable and do not depend on the $25,000,000 command-capacity workstream. Any command capacity must be released by approved use case, architecture, security test, consumption ceiling, and acceptance gate. A reduction must preserve inventories, risk tiering, testing, logging, evidence, and human approval.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

ESTIMATED IT COST

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$18,000,000	$23,500,000	$17,000,000	$17,000,000	$17,000,000	$92,500,000

SCALABILITY

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$0	$0	$0	$0	$0	$0

FTE

2026	2027	2028	2029	2030	2031	2032
0.0	0.0	0.0	0.0	0.0	0.0	0.0

DESCRIPTION OF ANTICIPATED OUT-YEAR COSTS :

The documented planning continuation is $17,000,000 annually for FY 2030 through FY 2032. Allocation among continuing workstreams remains subject to accepted demand, procurement, and consumption controls.

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$17,000,000	$17,000,000	$17,000,000
OUT-YEAR GR ONLY COSTS FOR ITEM:			
1 General Revenue Fund	$17,000,000	$17,000,000	$17,000,000
TOTAL OUT-YEAR GR ONLY:	$17,000,000	$17,000,000	$17,000,000

APPROXIMATE PERCENTAGE OF EXCEPTIONAL ITEM : 85.00%

CONTRACT DESCRIPTION :

Cryptographic discovery and transition planning; AI system inventory and assurance; model and agent testing; approved model access and compute; automation and engineering; identity, logging, evidence, human approval, data protection, monitoring, and consumption controls. Related implementation, integration, testing, training, support, and transition services may be procured.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029
	Item Name: ISAO: Information Sharing and Governance Modernization		
	Item Priority: 4		
	IT Component: Yes		
	Anticipated Out-year Costs: Yes		
	Involve Contracts > $50,000: Yes		
	Includes Funding for the Following Strategy or Strategies: 01-01-01 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	6,215,000	6,215,000
	TOTAL, OBJECT OF EXPENSE	**$6,215,000**	**$6,215,000**
METHOD OF FINANCING:			
1	General Revenue Fund	6,215,000	6,215,000
	TOTAL, METHOD OF FINANCING	**$6,215,000**	**$6,215,000**

DESCRIPTION / JUSTIFICATION:

Texas Cyber Command needs a single, trusted statewide capability to accelerate cyber risk decisions, secure cloud authorization, and deliver actionable information before vulnerabilities become incidents.

Current functions remain fragmented across manual workflows, separate records, contractor-supported assessments, and inconsistent information sharing, limiting speed, accountability, and statewide visibility.

Funding will establish the integrated information-sharing, governance, risk-management, and authorization capability required by Government Code Section 2063.204(a) to operate an ISAO serving state agencies, local governments, higher education, and the private sector. It will also support the standardized state risk and authorization management program required under Section 2063.408(b) and recurring security assessments and penetration testing required under Section 2063.409.

The $12,430,000 FY 2028-29 request includes $7,000,000 for governance and authorization workflow and $5,430,000 for assurance and trusted-sharing capacity.

Funding will integrate risk registers, security and application assessments, penetration-testing results, PCLS and TX-RAMP workflows, findings and remediation, control evidence, executive reporting, member onboarding, intake, triage, routing, and information dissemination.

The result is a governed statewide system of record that connects evidence to decisions and information to action.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

EXTERNAL/INTERNAL FACTORS:

External factors include cloud-service demand, provider and assessor capacity, changing authorization requirements, member participation, confidentiality and disclosure protections, and procurement timing.

Internal factors include an approved service catalog, member identity and access, records and evidence requirements, interfaces to incident intake and intelligence-product release, staffing classification and benefits, contractor transition, reconciliation of the existing ISAO and assurance base, and staged release of delivery capacity as demand is validated.

PCLS TRACKING KEY:

PCLS_90R_371_1971888

DESCRIPTION OF IT COMPONENT INCLUDED IN EXCEPTIONAL ITEM:

ISAO member identity, onboarding, intake, release and dissemination records; governance, risk, security assessment, authorization, continuous monitoring, findings, evidence, remediation, dashboards, reporting, and partner workflow.

IS THIS IT COMPONENT RELATED TO A NEW OR CURRENT PROJECT?

NEW

STATUS:

Planning and pre-procurement.

OUTCOMES:

Faster trusted dissemination, more consistent cloud-security decisions, shorter findings and remediation cycles, more reliable member onboarding, and auditable evidence and release records.

OUTPUTS:

Describe the program or system related performance objective and the measures that will gauge the project's success. Governance and authorization records; findings and remediation workflow; dashboards and reports; member onboarding and access records; sharing products and release logs; ISAO procedures; accepted staffing and contractor-transition plan; intelligence-product interfaces; and quarterly service reporting.

TYPE OF PROJECT

Cyber Security

ALTERNATIVE ANALYSIS

The $7,000,000 governance and authorization platform is an independently executable foundation. The $5,430,000 assurance and trusted-sharing delivery-capacity block adds member onboarding, cloud-assurance delivery, dissemination, partner support, and contractor transition. Either configuration must preserve disclosure, identity, evidence, audit, and release controls.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

ESTIMATED IT COST

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$6,215,000	$6,215,000	$0	$0	$0	$12,430,000

SCALABILITY

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$0	$0	$0	$0	$0	$0

FTE

2026	2027	2028	2029	2030	2031	2032
0.0	0.0	0.0	0.0	0.0	0.0	0.0

DESCRIPTION OF ANTICIPATED OUT-YEAR COSTS :

Out-year costs will reflect platform support, authorization and continuous-monitoring demand, member volume, in-house delivery capacity, contractor transition, and trusted-sharing operations as the operating model and demand are validated.

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$6,215,000	$6,215,000	$6,215,000
OUT-YEAR GR ONLY COSTS FOR ITEM:			
1 General Revenue Fund	$6,215,000	$6,215,000	$6,215,000
TOTAL OUT-YEAR GR ONLY:	$6,215,000	$6,215,000	$6,215,000

APPROXIMATE PERCENTAGE OF EXCEPTIONAL ITEM : 43.00%

CONTRACT DESCRIPTION :

ISAO member identity, onboarding, intake, release and dissemination records; governance, risk, security assessment, authorization, continuous monitoring, findings, evidence, remediation, dashboards, reporting, and partner workflow. Related implementation, integration, testing, training, support, and transition services may be procured.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION			Excp 2028	Excp 2029
	Item Name:	Earlier Warning for Texas Critical Infrastructure			
	Item Priority:	5			
	IT Component:	Yes			
	Anticipated Out-year Costs:	No			
	Involve Contracts > $50,000:	Yes			
	Includes Funding for the Following Strategy or Strategies:	01-01-01	Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:					
5000	CAPITAL EXPENDITURES			9,150,000	9,150,000
	TOTAL, OBJECT OF EXPENSE			**$9,150,000**	**$9,150,000**
METHOD OF FINANCING:					
1	General Revenue Fund			9,150,000	9,150,000
	TOTAL, METHOD OF FINANCING			**$9,150,000**	**$9,150,000**

DESCRIPTION / JUSTIFICATION:

Texas Government Code Chapter 2063 assigns the Texas Cyber Command (TXCC) responsibility for monitoring and coordinating cyber threat intelligence, detecting and warning of cyber attacks, and identifying threats to state systems and critical infrastructure.

The Cybersecurity Threat Intelligence Center (CTIC) serves as Texas' early-warning capability. TXCC's baseline budget provides foundational capability but is insufficient to provide the source governance, Texas-specific dependency analysis, collection prioritization, and analytic capacity needed for timely, decision-ready warning.

This $18,300,000 FY 2028-29 request includes $6,000,000 for bounded collection sensors, $10,000,000 for critical infrastructure decision support and analysis, $1,500,000 for threat data, and $800,000 for analyst training and mission travel.

Each source must be tied to an approved intelligence requirement, authority, owner, mission stakeholder, license, current-base comparison, and nonduplication finding.

The request funds intelligence requirements, analysis, products, warning, and collection governance. It does not duplicate shared operational telemetry or assume ownership of incident-execution records.

No new state FTE costs are included.

EXTERNAL/INTERNAL FACTORS:

External factors include federal and commercial source access, license restrictions, critical infrastructure participation, classification and handling requirements, rapidly changing adversary methods, and procurement lead times.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

Internal factors include approved intelligence requirements, collection governance, analyst capacity, source validation, data handling, product review, dissemination, feedback, and a line-level overlap crosswalk with shared operational services, regional delivery, and the current base.

Services provided to non-state entities remain subject to applicable authority and agreement.

PCLS TRACKING KEY:
PCLS_90R_371_1971881

DESCRIPTION OF IT COMPONENT INCLUDED IN EXCEPTIONAL ITEM:

Intelligence requirements, collection and source management, enrichment, critical infrastructure dependency analysis, production, review, warning, dissemination, and feedback capabilities.

IS THIS IT COMPONENT RELATED TO A NEW OR CURRENT PROJECT?
CURRENT

STATUS:
Planning and pre-procurement.

OUTCOMES:
Earlier, better-supported warning, stronger Texas-specific consequence analysis, more disciplined collection, and more timely decision support for governmental and critical infrastructure partners.

OUTPUTS:

Approved intelligence requirements; source, authority, license, owner, and consumer register; bounded collection; critical infrastructure dependency and consequence analysis; reviewed products and warnings; dissemination and feedback records; training; and quarterly timeliness, quality, use, and duplication reporting.

TYPE OF PROJECT
Cyber Security

ALTERNATIVE ANALYSIS

The $10,000,000 decision-support and analysis block can use current approved sources. The $1,500,000 threat-data and $6,000,000 collection blocks proceed only for documented intelligence requirements not met by current or shared services. The $800,000 training and mission-travel block scales to the accepted analyst operating model. Reduced funding must retain source governance, review, dissemination, and feedback controls.

ESTIMATED IT COST

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$9,150,000	$9,150,000	$0	$0	$0	$18,300,000

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029
SCALABILITY			

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$0	$0	$0	$0	$0	$0

FTE

2026	2027	2028	2029	2030	2031	2032
0.0	0.0	0.0	0.0	0.0	0.0	0.0

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$0	$0	$0

APPROXIMATE PERCENTAGE OF EXCEPTIONAL ITEM : 90.00%

CONTRACT DESCRIPTION :

Intelligence requirements, collection and source management, enrichment, critical infrastructure dependency analysis, production, review, warning, dissemination, and feedback capabilities. Related implementation, integration, testing, training, support, and transition services may be procured.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029
	Item Name: Rapid Cyber Incident Intake, Coordination, and Recovery		
	Item Priority: 6		
	IT Component: Yes		
	Anticipated Out-year Costs: Yes		
	Involve Contracts > $50,000: Yes		
	Includes Funding for the Following Strategy or Strategies: 02-01-01 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	6,800,000	6,800,000
	TOTAL, OBJECT OF EXPENSE	**$6,800,000**	**$6,800,000**
METHOD OF FINANCING:			
1	General Revenue Fund	6,800,000	6,800,000
	TOTAL, METHOD OF FINANCING	**$6,800,000**	**$6,800,000**

DESCRIPTION / JUSTIFICATION:

Texas Government Code Chapter 2063 requires the Texas Cyber Command (TXCC) to receive cyber incident reports, operate a 24-hour cyber reporting hotline for state agencies and covered entities, administer a statewide portal for cybersecurity incident management, and support entities experiencing cyber incidents.

Existing hotline, ticketing, collaboration, response, and partner channels do not maintain a single, tested record from initial contact through assignment, response, evidence handoff, recovery, follow-up analysis, and closure.

This $13,600,000 FY 2028-29 request includes $11,200,000 for the common incident portal and authoritative case service and $2,400,000 for hotline technology. The request includes identity, role, tenant, workflow, integration, audit, reporting, backup, export, and alternate-operation controls.

The Section 2063.302 reporting requirement is not extended beyond state agencies and local governments. The information-sharing function does not assume incident command or ownership of the authoritative record.

No new state FTE costs are included.

EXTERNAL/INTERNAL FACTORS:

External factors include incident volume, reporting obligations, participating-entity agreements, data sensitivity, accessibility, telecommunications availability, partner-system integration, and procurement timing.

Internal factors include an approved case model, intake and severity rules, identity and tenant design, response service levels, evidence and warning handoffs, records

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

retention, alternate operations, training, and acceptance exercises.

This request funds technology and a common workflow. Any additional 24-hour workforce requirements would require separate validation.

PCLS TRACKING KEY:

PCLS_90R_371_1971891

DESCRIPTION OF IT COMPONENT INCLUDED IN EXCEPTIONAL ITEM:

Statewide incident portal, hotline technology, authoritative case record, workflow, identity and tenant access, integrations, audit, reporting, backup, export, and alternate-operation capabilities.

IS THIS IT COMPONENT RELATED TO A NEW OR CURRENT PROJECT?

NEW

STATUS:

Planning and pre-procurement.

OUTCOMES:

Faster and more consistent intake, accountable mission assignment, coordinated response, accepted evidence handoffs, visible restoration status, and defensible closure and follow-up analysis.

OUTPUTS:

Production portal and authoritative incident record; 24-hour hotline technology; approved case, severity, routing, identity, tenant, audit, retention, export, and continuity controls; accepted evidence, warning, sharing, and regional interfaces; procedures; training; and quarterly service reporting.

TYPE OF PROJECT

Cyber Security

ALTERNATIVE ANALYSIS

The $11,200,000 portal and authoritative case service is an independently usable foundation. The $2,400,000 hotline technology block can be procured separately but must use the common identity, routing, audit, continuity, and case-integration controls. A reduced request must preserve one authoritative record and alternate operations.

ESTIMATED IT COST

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$6,800,000	$6,800,000	$0	$0	$0	$13,600,000

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

SCALABILITY

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$0	$0	$0	$0	$0	$0

FTE

2026	2027	2028	2029	2030	2031	2032
0.0	0.0	0.0	0.0	0.0	0.0	0.0

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$6,800,000	$6,800,000	$6,800,000

APPROXIMATE PERCENTAGE OF EXCEPTIONAL ITEM : 100.00%

CONTRACT DESCRIPTION :

Statewide incident portal, hotline technology, authoritative case record, workflow, identity and tenant access, integrations, audit, reporting, backup, export, and alternate-operation capabilities. Related implementation, integration, testing, training, support, and transition services may be procured.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION			Excp 2028	Excp 2029
	Item Name:	Shared Cyber Protection for Texas Government, RSOCs, and Partners			
	Item Priority:	7			
	IT Component:	Yes			
	Anticipated Out-year Costs:	Yes			
	Involve Contracts > $50,000:	Yes			
	Includes Funding for the Following Strategy or Strategies:	02-01-01	Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:					
5000	CAPITAL EXPENDITURES			39,800,000	25,800,000
	TOTAL, OBJECT OF EXPENSE			**$39,800,000**	**$25,800,000**
METHOD OF FINANCING:					
1	General Revenue Fund			39,800,000	25,800,000
	TOTAL, METHOD OF FINANCING			**$39,800,000**	**$25,800,000**

DESCRIPTION / JUSTIFICATION:

TXCC must implement consistent identity, digital trust, edge, Domain Name Service (DNS), cloud protection, and regional cyber defense services to carry out its network-security and cybersecurity-service responsibilities under Government Code Chapters 2059 and 2063.

Existing systems, provider arrangements, local practices, and regional delivery models provide uneven coverage and lack a common statewide service catalog, onboarding model, lifecycle controls, telemetry interfaces, support standards, and unit-cost basis.

This $65,600,000 FY 2028-29 request includes $12,300,000 for identity security, $7,700,000 for public and private certificate-authority services, $7,500,000 for managed edge and protective DNS, $7,100,000 for cloud posture and workload protection, and $31,000,000 for RSOC regional delivery and expansion.

The RSOC workstream funds interagency and interlocal agreements, additional regional operating capacity, onboarding to common TXCC services, common operating standards and procedures, service management and assurance, escalation and evidence handoffs, exercises, partner support, workforce participation, and sequenced expansion through eligible university-hosted centers.

The request does not fund duplicative identity, certificate, edge, DNS, cloud, sensor, case-management, or intelligence platforms. These are mission services for participating entities and RSOCs, not routine command-office IT.

Consistent with Section 2063.008, the request does not mandate a specific product. No new state FTE costs are included.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

EXTERNAL/INTERNAL FACTORS:

External factors include entity participation, identity and domain authority, provider markets, certificate trust, cloud adoption, connectivity, data handling, and procurement timing.

Internal factors include designated service owners, service catalogs, eligibility and agreements, onboarding, unit and pricing basis, integration architecture, telemetry routing, privacy, support coverage, cost recovery, continuity, and a line-level comparison to base and enterprise agreements.

Each service requires operational acceptance before statewide scaling.

PCLS TRACKING KEY:

PCLS_90R_371_1971889

DESCRIPTION OF IT COMPONENT INCLUDED IN EXCEPTIONAL ITEM:

Statewide identity security; public and private certificate lifecycle; managed edge and protective DNS; cloud posture and workload protection; RSOC agreements and regional operating capacity; common-service onboarding; service management and assurance; telemetry and case interfaces; common standards and procedures; exercises; continuity; and support.

IS THIS IT COMPONENT RELATED TO A NEW OR CURRENT PROJECT?

CURRENT

STATUS:

Planning and pre-procurement.

OUTCOMES:

Stronger identity control, managed digital trust, more consistent edge and DNS protection, improved cloud exposure and workload protection, expanded regional delivery capacity, and measurable service coverage, performance, and unit cost for approved participants and RSOCs.

OUTPUTS:

Service catalogs and eligibility rules; identity integrations and access reviews; certificate inventory and lifecycle records; managed edge and protective DNS deployments; cloud posture and workload coverage; RSOC agreements and expansion plans; common-service onboarding; approved standards and procedures; escalation and evidence handoffs; exercises; service assurance; support and continuity procedures; and quarterly adoption, performance, security, cost, and duplication reporting.

TYPE OF PROJECT

Cyber Security

ALTERNATIVE ANALYSIS

Identity security, certificate services, managed edge and protective DNS, cloud posture and workload protection, and RSOC regional delivery and expansion are distinct subrequests. They may be phased separately when service ownership, eligible cohorts, cost basis, integration, support, continuity, and acceptance criteria are complete. RSOC expansion must use common TXCC services and operating standards and may not rebuy duplicative identity, certificate, edge, DNS, cloud, sensor, case-management, or intelligence platforms. Routine command IT cannot be added to this request.

Agency code: **371** Agency name: **Texas Cyber Command**

CODE	DESCRIPTION	Excp 2028	Excp 2029

ESTIMATED IT COST

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$39,800,000	$25,800,000	$0	$0	$0	$65,600,000

SCALABILITY

2026	2027	2028	2029	2030	2031	2032	Total Over Life of Project
$0	$0	$0	$0	$0	$0	$0	$0

FTE

2026	2027	2028	2029	2030	2031	2032
0.0	0.0	0.0	0.0	0.0	0.0	0.0

ESTIMATED ANTICIPATED OUT-YEAR COSTS FOR ITEM:

	2030	2031	2032
OUT-YEAR ALL FUNDS:	$25,800,000	$25,800,000	$25,800,000

APPROXIMATE PERCENTAGE OF EXCEPTIONAL ITEM : 100.00%

CONTRACT DESCRIPTION :

Statewide identity security, public and private certificate lifecycle, managed edge and protective DNS, cloud posture and workload protection, RSOC interagency and interlocal agreements, regional operating capacity, common-service onboarding, service management and assurance, telemetry and case interfaces, common standards and procedures, exercises, continuity, and support. Related implementation, integration, testing, training, support, and transition services may be procured.

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Sustain Cybersecurity Services Transferred From DIR and Cost-Recovery Funding		
Allocation to Strategy:	2-1-1 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
2009	OTHER OPERATING EXPENSE	27,665,400	26,752,644
TOTAL, OBJECT OF EXPENSE		**$27,665,400**	**$26,752,644**
METHOD OF FINANCING:			
1	General Revenue Fund	27,665,400	26,752,644
TOTAL, METHOD OF FINANCING		**$27,665,400**	**$26,752,644**

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Workforce Capacity to Execute Statewide Cybersecurity Mandates		
Allocation to Strategy:	1-1-1 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	4,204,888	4,204,888
1002	OTHER PERSONNEL COSTS	63,073	63,073
TOTAL, OBJECT OF EXPENSE		**$4,267,961**	**$4,267,961**
METHOD OF FINANCING:			
1	General Revenue Fund	4,267,961	4,267,961
TOTAL, METHOD OF FINANCING		**$4,267,961**	**$4,267,961**
FULL-TIME EQUIVALENT POSITIONS (FTE):		35.0	35.0

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Workforce Capacity to Execute Statewide Cybersecurity Mandates		
Allocation to Strategy:	2-1-1 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	4,573,237	4,573,237
1002	OTHER PERSONNEL COSTS	68,598	68,598
TOTAL, OBJECT OF EXPENSE		**$4,641,835**	**$4,641,835**
METHOD OF FINANCING:			
1	General Revenue Fund	4,641,835	4,641,835
TOTAL, METHOD OF FINANCING		**$4,641,835**	**$4,641,835**
FULL-TIME EQUIVALENT POSITIONS (FTE):		36.0	36.0

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Workforce Capacity to Execute Statewide Cybersecurity Mandates		
Allocation to Strategy:	3-1-1 Transform Training and Education Programs Transferred from DIR to TX		
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	2,337,241	2,337,241
1002	OTHER PERSONNEL COSTS	35,059	35,059
TOTAL, OBJECT OF EXPENSE		**$2,372,300**	**$2,372,300**
METHOD OF FINANCING:			
1	General Revenue Fund	2,372,300	2,372,300
TOTAL, METHOD OF FINANCING		**$2,372,300**	**$2,372,300**
FULL-TIME EQUIVALENT POSITIONS (FTE):		19.0	19.0

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Workforce Capacity to Execute Statewide Cybersecurity Mandates		
Allocation to Strategy:	4-1-1 Central Administration		
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	3,237,509	3,237,509
1002	OTHER PERSONNEL COSTS	48,561	48,561
TOTAL, OBJECT OF EXPENSE		**$3,286,070**	**$3,286,070**
METHOD OF FINANCING:			
1	General Revenue Fund	3,286,070	3,286,070
TOTAL, METHOD OF FINANCING		**$3,286,070**	**$3,286,070**
FULL-TIME EQUIVALENT POSITIONS (FTE):		30.0	30.0

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Securing AI and Preparing Texas for Quantum Risk		
Allocation to Strategy:	1-1-1 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	18,000,000	23,500,000
TOTAL, OBJECT OF EXPENSE		**$18,000,000**	**$23,500,000**
METHOD OF FINANCING:			
1	General Revenue Fund	18,000,000	23,500,000
TOTAL, METHOD OF FINANCING		**$18,000,000**	**$23,500,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	ISAO: Information Sharing and Governance Modernization		
Allocation to Strategy:	1-1-1 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	6,215,000	6,215,000
TOTAL, OBJECT OF EXPENSE		**$6,215,000**	**$6,215,000**
METHOD OF FINANCING:			
1	General Revenue Fund	6,215,000	6,215,000
TOTAL, METHOD OF FINANCING		**$6,215,000**	**$6,215,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Earlier Warning for Texas Critical Infrastructure		
Allocation to Strategy:	1-1-1 Enable CTIC, ISAO, and DFL with Transformational Capabilities		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	9,150,000	9,150,000
TOTAL, OBJECT OF EXPENSE		**$9,150,000**	**$9,150,000**
METHOD OF FINANCING:			
1	General Revenue Fund	9,150,000	9,150,000
TOTAL, METHOD OF FINANCING		**$9,150,000**	**$9,150,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Rapid Cyber Incident Intake, Coordination, and Recovery		
Allocation to Strategy:	2-1-1 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	6,800,000	6,800,000
TOTAL, OBJECT OF EXPENSE		**$6,800,000**	**$6,800,000**
METHOD OF FINANCING:			
1	General Revenue Fund	6,800,000	6,800,000
TOTAL, METHOD OF FINANCING		**$6,800,000**	**$6,800,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Code	Description	Excp 2028	Excp 2029
Item Name:	Shared Cyber Protection for Texas Government, RSOCs, and Partners		
Allocation to Strategy:	2-1-1 Transform Cyber Incident Response Capabilities Transferred		
OBJECTS OF EXPENSE:			
5000	CAPITAL EXPENDITURES	39,800,000	25,800,000
TOTAL, OBJECT OF EXPENSE		**$39,800,000**	**$25,800,000**
METHOD OF FINANCING:			
1	General Revenue Fund	39,800,000	25,800,000
TOTAL, METHOD OF FINANCING		**$39,800,000**	**$25,800,000**

Agency Code: **371** Agency name: **Texas Cyber Command**

GOAL: 1 Enhance Texas' Cybersecurity Readiness

OBJECTIVE: 1 Build Out and Elevate Texas Cyber Command's "Prevent" Mission — Service Categories:

STRATEGY: 1 Enable CTIC, ISAO, and DFL with Transformational Capabilities — Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Excp 2028	Excp 2029
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	4,204,888	4,204,888
1002	OTHER PERSONNEL COSTS	63,073	63,073
5000	CAPITAL EXPENDITURES	33,365,000	38,865,000
	Total, Objects of Expense	**$37,632,961**	**$43,132,961**
METHOD OF FINANCING:			
1	General Revenue Fund	37,632,961	43,132,961
	Total, Method of Finance	**$37,632,961**	**$43,132,961**
FULL-TIME EQUIVALENT POSITIONS (FTE):		35.0	35.0

EXCEPTIONAL ITEM(S) INCLUDED IN STRATEGY:

Workforce Capacity to Execute Statewide Cybersecurity Mandates

Securing AI and Preparing Texas for Quantum Risk

ISAO: Information Sharing and Governance Modernization

Earlier Warning for Texas Critical Infrastructure

Agency Code: **371** Agency name: **Texas Cyber Command**

GOAL: 2 Boost the State of Texas Cyber Resilience

OBJECTIVE: 1 Respond to and Recover from Malicious Cyber Intrusions Service Categories:

STRATEGY: 1 Transform Cyber Incident Response Capabilities Transferred Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Excp 2028	Excp 2029
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	4,573,237	4,573,237
1002	OTHER PERSONNEL COSTS	68,598	68,598
2009	OTHER OPERATING EXPENSE	27,665,400	26,752,644
5000	CAPITAL EXPENDITURES	46,600,000	32,600,000
	Total, Objects of Expense	**$78,907,235**	**$63,994,479**
METHOD OF FINANCING:			
1	General Revenue Fund	78,907,235	63,994,479
	Total, Method of Finance	**$78,907,235**	**$63,994,479**
FULL-TIME EQUIVALENT POSITIONS (FTE):		36.0	36.0

EXCEPTIONAL ITEM(S) INCLUDED IN STRATEGY:

Sustain Cybersecurity Services Transferred From DIR and Cost-Recovery Funding

Workforce Capacity to Execute Statewide Cybersecurity Mandates

Rapid Cyber Incident Intake, Coordination, and Recovery

Shared Cyber Protection for Texas Government, RSOCs, and Partners

Agency Code: **371** Agency name: **Texas Cyber Command**

GOAL: 3 Catalyze Growth in Texas' Highly Skilled Cybersecurity Workforce

OBJECTIVE: 1 Facilitate Education and Training of a Future Cybersecurity Workforce Service Categories:

STRATEGY: 1 Transform Training and Education Programs Transferred from DIR to TXCC Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Excp 2028	Excp 2029
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	2,337,241	2,337,241
1002	OTHER PERSONNEL COSTS	35,059	35,059
	Total, Objects of Expense	**$2,372,300**	**$2,372,300**
METHOD OF FINANCING:			
1	General Revenue Fund	2,372,300	2,372,300
	Total, Method of Finance	**$2,372,300**	**$2,372,300**
FULL-TIME EQUIVALENT POSITIONS (FTE):		19.0	19.0

EXCEPTIONAL ITEM(S) INCLUDED IN STRATEGY:

Workforce Capacity to Execute Statewide Cybersecurity Mandates

Agency Code: **371** Agency name: **Texas Cyber Command**

GOAL: 4 Indirect Administration

OBJECTIVE: 1 Central Administration Service Categories:

STRATEGY: 1 Central Administration Service: 35 Income: A.2 Age: B.3

CODE	DESCRIPTION	Excp 2028	Excp 2029
OBJECTS OF EXPENSE:			
1001	SALARIES AND WAGES	3,237,509	3,237,509
1002	OTHER PERSONNEL COSTS	48,561	48,561
	Total, Objects of Expense	**$3,286,070**	**$3,286,070**
METHOD OF FINANCING:			
1	General Revenue Fund	3,286,070	3,286,070
	Total, Method of Finance	**$3,286,070**	**$3,286,070**
FULL-TIME EQUIVALENT POSITIONS (FTE):		30.0	30.0

EXCEPTIONAL ITEM(S) INCLUDED IN STRATEGY:

Workforce Capacity to Execute Statewide Cybersecurity Mandates

371 Texas Cyber Command - Capital Budget Impact by Project, OOE, and MOF (EI)

Capital Project Name - Exceptional Item	Strategy	LBB Account	MOF Type	MOF Code	FY 2028 EI	FY 2029 EI
Securing AI and Preparing Texas for Quantum Risk	A.1.1	5000	GR	0001	18,000,000	23,500,000
ISAO: Information Sharing and Governance Modernization	A.1.1	5000	GR	0001	6,215,000	6,215,000
Earlier Warning for Texas Critical Infrastructure	A.1.1	5000	GR	0001	9,150,000	9,150,000
Rapid Cyber Incident Intake, Coordination, and Recovery	B.1.1	5000	GR	0001	6,800,000	6,800,000
Shared Cyber Protection for Texas Government, RSOCs, and Partners	B.1.1	5000	GR	0001	39,800,000	25,800,000
Total Capital Project Exceptional Items					**$ 79,965,000**	**$ 71,465,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE		Est 2026	Bud 2027	BL 2028	BL 2029
5003 Repair or Rehabilitation of Buildings and Facilities					
1/1 Texas Cyber Command – George H. W. Bush State Office Building Office Space TFC Build Out					
OBJECTS OF EXPENSE					
Capital					
General 5000 CAPITAL EXPENDITURES		$0	$1,500,000	$0	$0
Capital Subtotal OOE, Project	1	$0	$1,500,000	$0	$0
Subtotal OOE, Project	1	**$0**	**$1,500,000**	**$0**	**$0**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$1,500,000	$0	$0
Capital Subtotal TOF, Project	1	$0	$1,500,000	$0	$0
Subtotal TOF, Project	1	**$0**	**$1,500,000**	**$0**	**$0**
2/2 UTSA Space Planning - Texas Cyber Command Facility Renovation / Fit-Out Project					
OBJECTS OF EXPENSE					
Capital					
General 5000 CAPITAL EXPENDITURES		$0	$5,000,000	$0	$0
Capital Subtotal OOE, Project	2	$0	$5,000,000	$0	$0
Subtotal OOE, Project	2	**$0**	**$5,000,000**	**$0**	**$0**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$5,000,000	$0	$0

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE	Est 2026	Bud 2027	BL 2028	BL 2029
Capital Subtotal TOF, Project 2	$0	$5,000,000	$0	$0
Subtotal TOF, Project 2	**$0**	**$5,000,000**	**$0**	**$0**
Capital Subtotal, Category 5003	$0	$6,500,000	$0	$0
Informational Subtotal, Category 5003				
Total, Category 5003	**$0**	**$6,500,000**	**$0**	**$0**
5005 Acquisition of Information Resource Technologies				
3/3 Texas Cyber Command Armis Centrix SOC Management				
OBJECTS OF EXPENSE				
Capital				
General 2009 OTHER OPERATING EXPENSE	$0	$996,082	$1,055,847	$1,119,198
Capital Subtotal OOE, Project 3	$0	$996,082	$1,055,847	$1,119,198
Subtotal OOE, Project 3	**$0**	**$996,082**	**$1,055,847**	**$1,119,198**
TYPE OF FINANCING				
Capital				
General CA 1 General Revenue Fund	$0	$996,082	$1,055,847	$1,119,198
Capital Subtotal TOF, Project 3	$0	$996,082	$1,055,847	$1,119,198
Subtotal TOF, Project 3	**$0**	**$996,082**	**$1,055,847**	**$1,119,198**
4/4 Texas Cyber Command Cyware Threat Intelligence Platform				
OBJECTS OF EXPENSE				
Capital				
General 2009 OTHER OPERATING EXPENSE	$0	$2,680,000	$2,000,000	$2,500,000

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE		Est 2026	Bud 2027	BL 2028	BL 2029
Capital Subtotal OOE, Project	4	$0	$2,680,000	$2,000,000	$2,500,000
Subtotal OOE, Project	4	**$0**	**$2,680,000**	**$2,000,000**	**$2,500,000**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$2,680,000	$2,000,000	$2,500,000
Capital Subtotal TOF, Project	4	$0	$2,680,000	$2,000,000	$2,500,000
Subtotal TOF, Project	4	**$0**	**$2,680,000**	**$2,000,000**	**$2,500,000**
5/5 Texas Cyber Command Armis Whole State Enterprise Agreement					
OBJECTS OF EXPENSE					
Capital					
General 2009 OTHER OPERATING EXPENSE		$0	$0	$4,600,000	$4,600,000
Capital Subtotal OOE, Project	5	$0	$0	$4,600,000	$4,600,000
Subtotal OOE, Project	5	**$0**	**$0**	**$4,600,000**	**$4,600,000**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$0	$4,600,000	$4,600,000
Capital Subtotal TOF, Project	5	$0	$0	$4,600,000	$4,600,000
Subtotal TOF, Project	5	**$0**	**$0**	**$4,600,000**	**$4,600,000**

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE	Est 2026	Bud 2027	BL 2028	BL 2029
Capital Subtotal, Category 5005	$0	$3,676,082	$7,655,847	$8,219,198
Informational Subtotal, Category 5005				
Total, Category 5005	**$0**	**$3,676,082**	**$7,655,847**	**$8,219,198**
9000 Cybersecurity				
6/6 Securing AI and Preparing Texas for Quantum Risk				
OBJECTS OF EXPENSE				
Capital				
General 5000 CAPITAL EXPENDITURES	$0	$0	$0	$0
Capital Subtotal OOE, Project 6	$0	$0	$0	$0
Subtotal OOE, Project 6	**$0**	**$0**	**$0**	**$0**
TYPE OF FINANCING				
Capital				
General CA 1 General Revenue Fund	$0	$0	$0	$0
Capital Subtotal TOF, Project 6	$0	$0	$0	$0
Subtotal TOF, Project 6	**$0**	**$0**	**$0**	**$0**
7/7 ISAO: Information Sharing and Governance Modernization				
OBJECTS OF EXPENSE				
Capital				
General 5000 CAPITAL EXPENDITURES	$0	$0	$0	$0
Capital Subtotal OOE, Project 7	$0	$0	$0	$0

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE	Est 2026	Bud 2027	BL 2028	BL 2029
Subtotal OOE, Project 7	**$0**	**$0**	**$0**	**$0**
TYPE OF FINANCING				
Capital				
General CA 1 General Revenue Fund	$0	$0	$0	$0
Capital Subtotal TOF, Project 7	$0	$0	$0	$0
Subtotal TOF, Project 7	**$0**	**$0**	**$0**	**$0**
8/8 Earlier Warning for Texas Critical Infrastructure				
OBJECTS OF EXPENSE				
Capital				
General 5000 CAPITAL EXPENDITURES	$0	$0	$0	$0
Capital Subtotal OOE, Project 8	$0	$0	$0	$0
Subtotal OOE, Project 8	**$0**	**$0**	**$0**	**$0**
TYPE OF FINANCING				
Capital				
General CA 1 General Revenue Fund	$0	$0	$0	$0
Capital Subtotal TOF, Project 8	$0	$0	$0	$0
Subtotal TOF, Project 8	**$0**	**$0**	**$0**	**$0**
9/9 Rapid Cyber Incident Intake, Coordination, and Recovery				
OBJECTS OF EXPENSE				
Capital				
General 5000 CAPITAL EXPENDITURES	$0	$0	$0	$0

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE		Est 2026	Bud 2027	BL 2028	BL 2029
Capital Subtotal OOE, Project	9	$0	$0	$0	$0
Subtotal OOE, Project	9	**$0**	**$0**	**$0**	**$0**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$0	$0	$0
Capital Subtotal TOF, Project	9	$0	$0	$0	$0
Subtotal TOF, Project	9	**$0**	**$0**	**$0**	**$0**
10/10 Shared Cyber Protection for Texas Government, RSOCs, and Partners					
OBJECTS OF EXPENSE					
Capital					
General 5000 CAPITAL EXPENDITURES		$0	$0	$0	$0
Capital Subtotal OOE, Project	10	$0	$0	$0	$0
Subtotal OOE, Project	10	**$0**	**$0**	**$0**	**$0**
TYPE OF FINANCING					
Capital					
General CA 1 General Revenue Fund		$0	$0	$0	$0
Capital Subtotal TOF, Project	10	$0	$0	$0	$0
Subtotal TOF, Project	10	**$0**	**$0**	**$0**	**$0**

Agency code: **371** Agency name: **Texas Cyber Command**

Category Code / Category Name *Project Sequence/Project Id/ Name* OOE / TOF / MOF CODE	Est 2026	Bud 2027	BL 2028	BL 2029
Capital Subtotal, Category 9000	$0	$0	$0	$0
Informational Subtotal, Category 9000				
Total, Category 9000	**$0**	**$0**	**$0**	**$0**
AGENCY TOTAL -CAPITAL	**$0**	**$10,176,082**	**$7,655,847**	**$8,219,198**
AGENCY TOTAL -INFORMATIONAL				
AGENCY TOTAL	**$0**	**$10,176,082**	**$7,655,847**	**$8,219,198**
METHOD OF FINANCING:				
Capital				
General 1 General Revenue Fund	$0	$10,176,082	$7,655,847	$8,219,198
Total, Method of Financing-Capital	$0	$10,176,082	$7,655,847	$8,219,198
Total, Method of Financing	**$0**	**$10,176,082**	**$7,655,847**	**$8,219,198**
TYPE OF FINANCING:				
Capital				
General CA CURRENT APPROPRIATIONS	$0	$10,176,082	$7,655,847	$8,219,198
Total, Type of Financing-Capital	$0	$10,176,082	$7,655,847	$8,219,198
Total,Type of Financing	**$0**	**$10,176,082**	**$7,655,847**	**$8,219,198**

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**5003**	Category Name:	**REPAIR OR REHABILITATION**
Project number:	**1**	Project Name:	**TXCC Capitol Space Build Out**

PROJECT DESCRIPTION

General Information

This capital project funds the tenant buildout of 2,665 square feet of unfinished shell office space on the 10th floor, Suite 10.700, of the George H. W. Bush State Office Building at 1801 Congress Avenue in Austin, Texas, for the Texas Cyber Command (TXCC).

The Texas Facilities Commission formally offered the space on July 16, 2026. The space is currently in raw shell condition, and TXCC is responsible for the design and construction costs required to convert it into functional office space.

The purpose of the project is to create dedicated, purpose-configured workspace for TXCC within the Capitol Complex. The project addresses the agency's operational need for secure, efficient office facilities that support staff co-location, interagency coordination, and public affairs functions.

Completing the buildout will transform the offered shell space into usable offices tailored to TXCC's operational requirements. The time-limited nature of the space offer and the availability of unfinished space make the project necessary to secure the location and begin design and construction in a timely manner.

PLCS Tracking Key	N/A
Number of Units / Average Unit Cost	N/A
Estimated Completion Date	Fiscal Year 2027

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	0	0

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	$1,500,000
Estimated/Actual Project Cost	$1,500,000
Length of Financing/ Lease Period	N/A – Project is planned for completion in FY 2027.

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	**MOF_CODE**	**AVERAGE_AMOUNT**

Explanation: TXCC needs dedicated office space in the Capitol Complex to securely co-locate staff, support daily operations, protect sensitive work, and enable close coordination with state agency partners. The 2,665 SF shell space provides a centralized, customizable solution.

Project Location: George H. W. Bush State Office Building 10th floor Suite 10.700 1801 Congress Avenue, Austin, Texas

Beneficiaries: TXCC gains secure, purpose-built office space for efficient operations and staff co-location, while state agencies gain stronger Capitol Complex collaboration, coordination, and service delivery.

Frequency of Use and External Factors Affecting Use:

The office will support continuous, daily TXCC operations. Key factors include TFC's time-sensitive offer, statutory duties, secure Capitol Complex co-location, and stronger interagency collaboration.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**5003**	Category Name:	**REPAIR OR REHABILITATION**
Project number:	**2**	Project Name:	**TXCC UTSA San Pedro I Renovation**

PROJECT DESCRIPTION

General Information

This capital project renovates and finishes space in the University of Texas at San Antonio's San Pedro I building to serve as the operational headquarters for the Texas Cyber Command (TXCC).

The project will finish shell space, refresh existing Level 5 office areas, upgrade Level 1 conference and non-conference suites, improve the elevator lobby, and provide furniture, fixtures, and equipment. Work includes construction finish-out, light renovation, related contingencies, design, and project management.

The completed space will provide functional, secure workspace for TXCC's growing staff and support core cybersecurity operations. TXCC was established under Texas Government Code Chapter 2063 to prevent and respond to cyber incidents affecting state agencies, local governments, and critical infrastructure.

TXCC currently occupies temporary space in San Pedro I. The renovation will address insufficient finished offices, collaboration areas, and support spaces needed for threat intelligence, incident response, digital forensics, training, and interagency coordination.

San Antonio was selected as the headquarters location because of its concentration of cybersecurity expertise and existing federal and military partners. Completing the buildout will allow TXCC to fully establish its statutory functions without facility constraints and support the efficient, secure delivery of statewide cybersecurity services.

PLCS Tracking Key	N/A
Number of Units / Average Unit Cost	N/A
Estimated Completion Date	Fiscal Year 2027

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	0	0

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	20-35 Years
Estimated/Actual Project Cost	$5,000,000
Length of Financing/ Lease Period	N/A – Project is planned for completion in FY 2027.

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: TXCC currently operates in unfinished and under-configured temporary space in UTSA's San Pedro I building, which lacks adequate offices, collaboration areas, and workstations needed for staff growth and core functions. Renovating and finishing the existing space is the most efficient solution—leveraging the current location and partnership rather than seeking new facilities. Without it, TXCC cannot fully stand up operations, or deliver statutory cyber defense services on schedule.

Project Location: San Pedro I - Dolorosa Street San Antonio , Texas 78204

Beneficiaries: TXCC staff , state agencies, local governments, and critical infrastructure operators.

Frequency of Use and External Factors Affecting Use:

The renovated space will be used continuously for TXCC operations. External factors include statutory requirements, rising cybersecurity threats, and projected staff growth.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**5005**	Category Name:	**ACQUISITN INFO RES TECH.**
Project number:	**3**	Project Name:	**Armis Centrix SOC Management**

PROJECT DESCRIPTION

General Information

This project funds Armis Centrix SOC Management licensing and support for FY 2028-29. The capability supports the Texas Cyber Command (TXCC) in administering authorized, scoped, and segregated asset and exposure information, organizing coverage, identifying material exposure, and prioritizing operational response.

The project does not replace participating entities' responsibility for their own systems, authorize unrestricted collection of entity data, or duplicate the statewide enterprise license.

The separate Armis Whole State Enterprise project provides broader approved coverage. This project supports the SOC management capability used to manage, segment, and operationalize that coverage.

PLCS Tracking Key	N/A
Number of Units / Average Unit Cost	Enterprise subscription
Estimated Completion Date	8/31/2029

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	1,119,199	1,119,199

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Ongoing annual service, subject to appropriation
Estimated/Actual Project Cost	$5,409,525
Length of Financing/ Lease Period	Annual General Revenue funding; no lease financing

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: Sustains the SOC management layer that converts authorized Armis asset and exposure visibility into prioritized action. It is separate from the statewide enterprise license and supports administration, segmentation, and operational use.

Project Location: TXCC-managed cloud service used by authorized TXCC and participating regional or entity personnel; no single physical project location.

Beneficiaries: State agencies and participating covered entities, plus the Texans and communities that depend on reliable government and critical services.

Frequency of Use and External Factors Affecting Use:

Used continuously for exposure review, prioritization, and incident support. Demand varies with onboarding, asset change, vulnerabilities, and cyber incidents.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**5005**	Category Name:	**ACQUISITN INFO RES TECH.**
Project number:	**4**	Project Name:	**Cyware Threat Intelligence**

PROJECT DESCRIPTION

General Information

This project funds the Cyware threat intelligence platform and associated support for FY 2028-29. The capability supports controlled information exchange, enrichment, requests for information, collaboration, and dissemination of authorized, shareable intelligence.

Cyware helps convert relevant intelligence into warnings, advisories, detections, hunts, and partner action. The project does not make Cyware the repository for raw incident evidence, unrestricted case records, or all operational telemetry.

Access to the platform and the information it contains remains governed by applicable authority, operational need, and information-sharing restrictions.

PLCS Tracking Key	N/A
Number of Units / Average Unit Cost	Enterprise subscription
Estimated Completion Date	8/31/2029

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	2,500,000	2,500,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Ongoing annual service, subject to appropriation
Estimated/Actual Project Cost	$12,180,000
Length of Financing/ Lease Period	Annual General Revenue funding; no lease financing

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: Sustains the controlled exchange and workflow platform that moves authorized threat intelligence from receipt and enrichment to warnings, advisories, detections, hunts, and partner action.

Project Location: TXCC-managed cloud service used by authorized TXCC, regional, state, local, higher education, and private-sector participants.

Beneficiaries: State agencies, local governments, higher education, approved private-sector partners, and Texans who rely on secure and resilient services.

Frequency of Use and External Factors Affecting Use:

Used continuously for intelligence receipt, enrichment, coordination, and dissemination. Use rises with new threats, incidents, and partner requests.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**5005**	Category Name:	**ACQUISITN INFO RES TECH.**
Project number:	**5**	Project Name:	**Armis Whole State Enterprise**

PROJECT DESCRIPTION

General Information

This project funds the Armis Whole State Enterprise agreement and associated support for FY 2028-29. The capability expands authorized asset and exposure visibility across approved state and partner environments, including information technology, operational technology, and Internet of Things assets.

Information remains entity-authorized, appropriately scoped, and segregated. The project does not replace local security ownership or require participation.

This project is separate from Armis Centrix SOC Management. The Whole State Enterprise agreement provides broader approved coverage, while Centrix provides the SOC management layer used to administer and operationalize that coverage.

PLCS Tracking Key	N/A
Number of Units / Average Unit Cost	Enterprise subscription
Estimated Completion Date	8/31/2029

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	4,600,000	4,600,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Ongoing annual service, subject to appropriation
Estimated/Actual Project Cost	$18,400,000
Length of Financing/ Lease Period	Annual General Revenue funding; no lease financing

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	**MOF_CODE**	**AVERAGE_AMOUNT**

Explanation: Expands authorized enterprise asset and exposure visibility across approved participants while preserving local ownership, entity scope, and segmentation. It is separate from the Centrix SOC management layer.

Project Location: Cloud service supporting authorized participating environments across Texas; no single physical project location.

Beneficiaries: Approved state and covered entities, regional partners, and Texans whose communities depend on reliable government and critical infrastructure services.

Frequency of Use and External Factors Affecting Use:

Used continuously as authorized assets, exposures, and vulnerabilities change. Demand grows with partner onboarding, technology change, and incidents.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**9000**	Category Name:	**Cybersecurity**
Project number:	**6**	Project Name:	**AI and Quantum Risk**

PROJECT DESCRIPTION

General Information

This project establishes new statewide cybersecurity technology capabilities to address emerging risks associated with artificial intelligence and quantum computing. The project includes development of a statewide cryptographic inventory and post-quantum readiness program, an AI security and assurance capability, and controlled technology capacity to support AI-assisted cyber defense.

Project activities include cryptographic discovery, cryptographic bills of materials, risk and readiness assessments, standards and pilots, AI asset discovery, architecture review, model and artifact scanning, security testing, data-leakage controls, runtime monitoring, approved model access, compute, automation, and related engineering.

The total FY 2028–29 project request is $41,500,000, consisting of $25,000,000 for AI model access, compute, automation, and engineering; $10,000,000 for statewide AI system security and assurance; and $6,500,000 for cryptographic discovery and post-quantum readiness.

The project is intended to establish governed, scalable, and auditable cybersecurity capabilities and does not include general AI application development or wholesale replacement of existing cryptographic systems.

PLCS Tracking Key	PCLS_90R_371_1971890
Number of Units / Average Unit Cost	FY 2028–32 Total: $92.5M | Avg. Annual Cost: $18.5M
Estimated Completion Date	TBD

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	17,000,000	17,000,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Aprox. 5 years or more
Estimated/Actual Project Cost	$92,510,150
Length of Financing/ Lease Period	N/A

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: This new cybersecurity project addresses statewide readiness gaps for artificial intelligence and emerging quantum-computing risks. Funding establishes governed capabilities for post-quantum readiness, AI security and assurance, and controlled AI model access, compute, automation, and engineering, with appropriate security, logging, evidence, monitoring, and approval controls.

Project Location: Statewide – Texas Cyber Command and participating state entities.

Beneficiaries: Texas Cyber Command, state agencies, and eligible public-sector partners statewide.

Frequency of Use and External Factors Affecting Use:

Use will be ongoing and will vary based on approved AI use cases, model and compute demand, cryptographic readiness activities, and evolving security requirements. External factors include standards maturity, vendor cryptographic roadmaps, model and agent changes, provider terms, export and data-location constraints, procurement timing, and uncertain consumption.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**9000**	Category Name:	**Cybersecurity**
Project number:	**7**	Project Name:	**ISAO Governance Modernization**

PROJECT DESCRIPTION

General Information

This project establishes an integrated statewide information-sharing, governance, risk-management, and authorization capability for Texas Cyber Command. It will support ISAO operations, standardized risk and authorization management, recurring security assessments, and penetration testing.

The project will integrate risk registers, assessments, PCLS and TX-RAMP workflows, findings and remediation, control evidence, executive reporting, member onboarding, intake, triage, routing, and information dissemination into a governed statewide system of record.

PLCS Tracking Key	PCLS_90R_371_1971888
Number of Units / Average Unit Cost	FY 2028–29 Total: $31.1M | Avg. Annual Cost: $6.215M
Estimated Completion Date	TBD

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	6,215,000	6,215,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Aprox 5 years or more
Estimated/Actual Project Cost	$31,075,000
Length of Financing/ Lease Period	N/A

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: This project addresses fragmented information-sharing, governance, risk-management, and authorization processes that limit speed, consistency, accountability, and statewide visibility. Funding will establish a governed statewide system of record that connects assessments, evidence, findings, remediation, authorization decisions, member onboarding, and information dissemination to support faster and more consistent cybersecurity decisions.

Project Location: Statewide – Texas Cyber Command and participating state agencies, local governments, higher education institutions, and other eligible partners.

Beneficiaries: State agencies, local governments, higher education, private-sector partners, and other eligible entities using TXCC cybersecurity services.

Frequency of Use and External Factors Affecting Use:

Use will be ongoing and will vary with cloud-service demand, authorization activity, member participation, provider and assessor capacity, changing requirements, confidentiality protections, and procurement timing.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**9000**	Category Name:	**Cybersecurity**
Project number:	**8**	Project Name:	**CTIC Threat Warning**

PROJECT DESCRIPTION

General Information

This project strengthens the Texas Cyber Command's Cybersecurity Threat Intelligence Center (CTIC) by expanding statewide cyber threat collection, analysis, and early-warning capabilities for state systems and critical infrastructure.

Funding will support bounded collection sensors, critical infrastructure decision support and analysis, threat data, and analyst training. The project will improve source governance, collection prioritization, Texas-specific dependency analysis, and the delivery of timely, decision-ready cyber threat intelligence.

The FY 2028–29 project request totals $18,300,000 and is designed to complement existing operational capabilities without duplicating shared telemetry or incident-management functions.

PLCS Tracking Key	PCLS_90R_371_1971881
Number of Units / Average Unit Cost	FY 2028–29 Total: $18.3M | Avg. Annual Cost: $9.15M
Estimated Completion Date	TBD

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	0	0

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Aprox. 5 years or more
Estimated/Actual Project Cost	$18,300,000
Length of Financing/ Lease Period	N/A

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: This project addresses gaps in statewide cyber threat collection, source governance, critical infrastructure analysis, and early-warning capacity. Funding will improve collection prioritization, Texas-specific dependency analysis, threat-data access, and analytic capability to support timely, decision-ready warnings for state systems and critical infrastructure.

Project Location: Statewide – Texas Cyber Command and participating state agencies, critical infrastructure partners, and other eligible entities across Texas.

Beneficiaries: State agencies, critical infrastructure partners, local governments, and other eligible entities that rely on TXCC cyber threat intelligence and early-warning services.

Frequency of Use and External Factors Affecting Use:

Use will be ongoing and will vary based on threat activity, intelligence requirements, source availability, critical infrastructure participation, and operational demand. External factors include federal and commercial source access, license restrictions, classification and handling requirements, changing adversary methods, and procurement lead times.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**9000**	Category Name:	**Cybersecurity**
Project number:	**9**	Project Name:	**Incident Intake and Recovery**

PROJECT DESCRIPTION

General Information

This project establishes a statewide cyber incident intake, coordination, and case-management capability for the Texas Cyber Command. It will support the 24-hour cyber reporting hotline and statewide cybersecurity incident management portal.

Funding will provide a common incident portal, authoritative case service, hotline technology, and supporting identity, access, workflow, integration, audit, reporting, backup, export, and alternate-operation controls.

The FY 2028–29 project request totals $13,600,000 and is intended to create a consistent, secure record from initial incident reporting through assignment, response, evidence handoff, recovery, follow-up, and closure.

PLCS Tracking Key	PCLS_90R_371_1971891
Number of Units / Average Unit Cost	FY 2028–29 Total: $34M | Avg. Annual Cost: $6.8M
Estimated Completion Date	TBD

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	6,800,000	6,800,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Aprox. 5 years or more
Estimated/Actual Project Cost	$34,000,000
Length of Financing/ Lease Period	N/A

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: This project addresses fragmented incident intake, reporting, coordination, and case-management processes that limit consistency, accountability, and statewide visibility. Funding will establish a common portal, authoritative case record, and hotline technology to support secure incident tracking from initial report through response, evidence handoff, recovery, follow-up, and closure.

Project Location: Statewide – Texas Cyber Command and participating state agencies, local governments, covered entities, and other eligible partners across Texas.

Beneficiaries: State agencies, local governments, covered entities, and other eligible partners that rely on TXCC for cyber incident reporting, coordination, response, and recovery support.

Frequency of Use and External Factors Affecting Use:

Use will be ongoing and will vary based on incident volume, reporting obligations, participating-entity demand, and operational needs. External factors include data sensitivity, telecommunications availability, partner-system integration, participating-entity agreements, accessibility requirements, and procurement timing.

Agency Code:	**371**	Agency name:	**Texas Cyber Command**
Category Number:	**9000**	Category Name:	**Cybersecurity**
Project number:	**10**	Project Name:	**Shared Cyber Protection**

PROJECT DESCRIPTION

General Information

This project establishes consistent statewide identity, digital trust, edge, Domain Name Service (DNS), cloud protection, and regional cyber defense capabilities for Texas Cyber Command and participating entities.

Funding will support identity security, certificate-authority services, managed edge and protective DNS, cloud posture and workload protection, and Regional Security Operations Center (RSOC) delivery and expansion.

The FY 2028–29 project request totals $65,600,000 and is intended to improve statewide coverage through common service standards, onboarding, lifecycle controls, telemetry interfaces, support processes, and coordinated regional delivery without duplicating existing cybersecurity platforms.

PLCS Tracking Key	PCLS_90R_371_1971889
Number of Units / Average Unit Cost	FY 2028–29 Total: $143M | Avg. Annual Cost: $26.8M
Estimated Completion Date	TBD

Additional Capital Expenditure Amounts Required	**2030**	**2031**
	25,800,000	25,800,000

Type of Financing	CA CURRENT APPROPRIATIONS
Projected Useful Life	Aprox. 5 years or more
Estimated/Actual Project Cost	$143,000,000
Length of Financing/ Lease Period	N/A

ESTIMATED/ACTUAL DEBT OBLIGATION PAYMENTS

2028	**2029**	**2030**	**2031**	**Total over project life**
0	0	0	0	0

REVENUE GENERATION / COST SAVINGS

REVENUE_COST_FLAG	MOF_CODE	AVERAGE_AMOUNT

Explanation: This project addresses uneven statewide coverage and fragmented service delivery across identity, digital trust, edge, DNS, cloud protection, and regional cyber defense. Funding will establish common service standards, onboarding, lifecycle controls, telemetry interfaces, support processes, and coordinated RSOC delivery to improve consistency, scalability, and statewide cybersecurity protection.

Project Location: Statewide – Texas Cyber Command, participating state entities, Regional Security Operations Centers (RSOCs), and eligible university-hosted regional partners across Texas.

Beneficiaries: State agencies, RSOCs, higher education institutions, local governments, and other eligible entities participating in TXCC shared cybersecurity and regional defense services.

Frequency of Use and External Factors Affecting Use:

Use will be ongoing and will vary based on entity participation, service demand, cloud adoption, and regional operational needs. External factors include identity and domain authority, provider markets, certificate trust, connectivity, data-handling requirements, and procurement timing.

371 Texas Cyber Command

Category Code / Category Name *Project Number / Name* OOE / TOF / MOF CODE	Excp 2028	Excp 2029
9000 Cybersecurity		
6 AI and Quantum Risk		
Objects of Expense		
5000 CAPITAL EXPENDITURES	18,000,000	23,500,000
Subtotal OOE, Project 6	**18,000,000**	**23,500,000**
Type of Financing		
CA 1 General Revenue Fund	18,000,000	23,500,000
Subtotal TOF, Project 6	**18,000,000**	**23,500,000**
7 ISAO Governance Modernization		
Objects of Expense		
5000 CAPITAL EXPENDITURES	6,215,000	6,215,000
Subtotal OOE, Project 7	**6,215,000**	**6,215,000**
Type of Financing		
CA 1 General Revenue Fund	6,215,000	6,215,000
Subtotal TOF, Project 7	**6,215,000**	**6,215,000**
8 CTIC Threat Warning		
Objects of Expense		
5000 CAPITAL EXPENDITURES	9,150,000	9,150,000
Subtotal OOE, Project 8	**9,150,000**	**9,150,000**
Type of Financing		
CA 1 General Revenue Fund	9,150,000	9,150,000
Subtotal TOF, Project 8	**9,150,000**	**9,150,000**
9 Incident Intake and Recovery		
Objects of Expense		
5000 CAPITAL EXPENDITURES	6,800,000	6,800,000

371 Texas Cyber Command

Category Code / Category Name *Project Number / Name* OOE / TOF / MOF CODE		Excp 2028	Excp 2029
Subtotal OOE, Project	9	**6,800,000**	**6,800,000**
Type of Financing			
CA 1 General Revenue Fund		6,800,000	6,800,000
Subtotal TOF, Project	9	**6,800,000**	**6,800,000**
10 Shared Cyber Protection			
Objects of Expense			
5000 CAPITAL EXPENDITURES		39,800,000	25,800,000
Subtotal OOE, Project	10	**39,800,000**	**25,800,000**
Type of Financing			
CA 1 General Revenue Fund		39,800,000	25,800,000
Subtotal TOF, Project	10	**39,800,000**	**25,800,000**
Subtotal Category	**9000**	**79,965,000**	**71,465,000**
AGENCY TOTAL		**79,965,000**	**71,465,000**
METHOD OF FINANCING:			
1 General Revenue Fund		79,965,000	71,465,000
Total, Method of Financing		**79,965,000**	**71,465,000**
TYPE OF FINANCING:			
CA CURRENT APPROPRIATIONS		79,965,000	71,465,000
Total,Type of Financing		**79,965,000**	**71,465,000**

6.B. Current Biennium Onetime Expenditure Schedule
Summary of Onetime Expenditures

Agency Code:	Agency Name:	Prepared By:	Date:
371	Texas Cyber Command	Sami Chadli	August 18, 2026

Projects	Estimated 2026	Budgeted 2027	Requested 2028	Requested 2029
TXCC Capitol Space Build Out	$0	$1,500,000	$1,500,000	$0
TXCC UTSA San Pedro I Renovation	$0	$5,000,000	$5,000,000	$0
Total, All Projects	$0	$6,500,000	$6,500,000	$0

6.B. Current Biennium Onetime Expenditure Schedule
Strategy Allocation from 2026-27 Biennium to 2028-29 Biennium

Agency Code:	Agency Name:	Prepared By:	Date:
371	Texas Cyber Command	Sami Chadli	August 18, 2026

2026-27		2028-29	
PROJECT:	TXCC Capitol Space Build Out	**PROJECT:**	Google SecOps Enterprise Plus
ALLOCATION TO STRATEGY: 4.1.1		**ALLOCATION TO STRATEGY:** 1.1.1	

Strategy Code	OOE/MOF Code	Strategy Allocation	Estimated 2026	Budgeted 2027	Requested 2028	Requested 2029
		Object of Expense:				
D.1.1	5000	Capital Expenditures	$0	$1,500,000	$1,500,000	$0
		Total, Object of Expense	$0	$1,500,000	$1,500,000	$0
		Method of Financing:				
D.1.1	0001	General Revenue	$0	$1,500,000	$1,500,000	$0
		Total, Method of Financing	$0	$1,500,000	$1,500,000	$0

Project Description for the 2026-27 Biennium:

Texas Cyber Command – George H. W. Bush State Office Building Office Space TFC Build Out.

Project Description and Allocation Purpose for the 2028-29 Biennium:

The $1.5 million partially covers $2.9 million for security operations enhancements through advanced threat detection, analysis, and automated response (Google SecOps Enterprise Plus).

6.B. Current Biennium Onetime Expenditure Schedule
Strategy Allocation from 2026-27 Biennium to 2028-29 Biennium

Agency Code:	Agency Name:	Prepared By:	Date:
371	Texas Cyber Command	Sami Chadli	August 18, 2026

2026-27		2028-29	
PROJECT:	TXCC UTSA San Pedro I Renovation	**PROJECT:**	Google SecOps Enterprise Plus Intrusion.com Software and Services
ALLOCATION TO STRATEGY: 4.1.1		**ALLOCATION TO STRATEGY: 1**.1.1	

Strategy Code	OOE/MOF Code	Strategy Allocation	Estimated 2026	Budgeted 2027	Requested 2028	Requested 2029
		Object of Expense:				
D.1.1	5000	Capital Expenditures	$0	$5,000,000	$5,000,000	$0
		Total, Object of Expense	$0	$5,000,000	$5,000,000	$0
		Method of Financing:				
D.1.1	0001	General Revenue	$0	$5,000,000	$5,000,000	$0
		Total, Method of Financing	$0	$5,000,000	$5,000,000	$0

Project Description for the 2026-27 Biennium:

UTSA Space Planning - Texas Cyber Command Facility Renovation / Fit-Out Project.

Project Description and Allocation Purpose for the 2028-29 Biennium:

The $5 million covers the remaining $1.4 million from Google SecOps Enterprise Plus and $3.6 million to enhance cyber threat intelligence and real-time network threat prevention capabilities (Intrusion.com Software and Services).

6.E. Estimated Revenue Collections Supporting Schedule

90th Regular Session, Agency Submission, Version 1

Automated Budget and Evaluation System of Texas (ABEST)

Agency Code: **371** Agency name: **Texas Cyber Command**

FUND/ACCOUNT	Act 2025	Exp 2026	Est 2027	Est 2028	Est 2029
1 General Revenue Fund					
Beginning Balance (Unencumbered):	$0	$0	$0	$0	$0
Estimated Revenue:					
Ending Fund/Account Balance	**$0**	**$0**	**$0**	**$0**	**$0**

REVENUE ASSUMPTIONS:

No revenues are to be collected for TXCC for fiscal 2026 through 2028.

CONTACT PERSON:

Sami Chadli

Agency Code: **371** Agency: **Texas Cyber Command**

EXECUTIVE ADVISORY GROUP

Statutory Authorization: Tex.Gov. Code sec. 2063.004(b)(2)
Number of Members: 10
Committee Status: New
Date Created: 1/23/2026
Date to Be Abolished: 9/1/2030

Strategy (Strategies):
1-1-1 ENABLE TRANSFORMATIONAL CAPABILITY
2-1-1 TRANSFORM CYBER IR CAPABILITIES
3-1-1 TRANSFORM TRAINING PROGRAMS
4-1-1 CENTRAL ADMINISTRATION

Advisory Committee Costs	**Expended Exp 2025**	**Estimated Est 2026**	**Budgeted Bud 2027**	**Requested BL 2028**	**Requested BL 2029**
Committee Members Direct Expenses					
Travel	$0	$21,750	$22,000	$22,000	$22,000
Rent - Building	0	4,059	5,000	5,000	5,000
Professional Fees & Services	0	253,906	220,000	220,000	220,000
Other Operating Expense	0	1,256	1,500	1,500	1,500
Total, Committee Expenditures	**$0**	**$280,971**	**$248,500**	**$248,500**	**$248,500**
Method of Financing					
General Revenue Fund	$0	$280,971	$248,500	$248,500	$248,500
Total, Method of Financing	**$0**	**$280,971**	**$248,500**	**$248,500**	**$248,500**
Meetings Per Fiscal Year	0	4	4	4	4

Agency Code: **371** Agency: **Texas Cyber Command**

Description and Justification for Continuation/Consequences of Abolishing

Advises TXCC on topics related to cyber security.