TEXAS CYBER COMMAND
STRATEGIC PLAN

Fiscal Years 2027 to 2031

Agency Strategic Plan
Fiscal Years 2027-2031

BY

TEXAS CYBER COMMAND

506 Dolorosa Street
San Antonio, Texas 78204

Date of Submission

Signed: 31 May 2026

Approved:

TABLE OF CONTENTS

Agency Strategic Plan

The Texas Cyber Command (TXCC) was formally established by the 89th Texas Legislature through House Bill 150, codified in Chapter 2063 of the Texas Government Code, with the mission to prevent and respond to cybersecurity incidents that affect state governmental entities and critical infrastructure in Texas. TXCC is a state agency governed by a Chief appointed by the Governor and confirmed by the Senate. Under the Chief's direction, the Command leads and coordinates the state cybersecurity program within the authorities, responsibilities, and legal guardrails established by law. The state cybersecurity program includes the policies, standards, procedures, structure, strategies, first principles design and governing architecture, objectives, plans, metrics, reports, services, and resources that establish the cybersecurity function for Texas.

As a newly established agency headquartered in San Antonio, TXCC is building the people, processes, partnerships, and technologies needed to protect essential public services, strengthen Texas's ability to anticipate, and withstand evolving cyber threats while reinforcing public trust.

Pursuant to Chapter 2063 of the Texas Government Code, TXCC is responsible for:

1. Providing leadership, guidance, and tools to enhance cybersecurity defenses;
2. Facilitating the education and training of a cybersecurity workforce;
3. Monitoring and coordinating cyber threat intelligence and information systems to detect and warn entities of cyberattacks, identifying cybersecurity threats to critical infrastructure and state systems, planning and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity to support law enforcement and attribute incidents;
4. Creating partnerships needed to effectively carry out the Command's functions; and
5. Receiving all cybersecurity incident reports from state agencies and covered entities.

The Command's general powers and duties are to:

1. Promote public awareness of cybersecurity issues;
2. Develop cybersecurity best practices and minimum standards for governmental entities;
3. Develop and provide training to state agencies and covered entities on cybersecurity measures and awareness;
4. Administer the cybersecurity threat intelligence center under Section 2063.201;
5. Provide support to state agencies and covered entities experiencing a cybersecurity incident and respond to cybersecurity reports received under Subchapter D and other reports as appropriate;
6. Administer the digital forensics laboratory under Section 2063.203;
7. Administer a statewide portal for enterprise cybersecurity threat, risk, and incident management, and operate a cybersecurity hotline available for state agencies and covered entities 24 hours a day, seven days a week;
8. Collaborate with law enforcement agencies to provide training and support related to cybersecurity incidents;

9. Serve as a clearinghouse for information relating to all aspects of protecting the cybersecurity of governmental entities, including sharing appropriate intelligence and information with governmental entities, federal agencies, and covered entities;
10. Collaborate with the Department of Information Resources (DIR) to ensure information resources and information resources technologies obtained by the department meet the cybersecurity standards and requirements;
11. Offer cybersecurity resources to state agencies and covered entities as determined by the Command;
12. Adopt policies to ensure state agencies implement sufficient cybersecurity measures to defend information resources, information resources technologies, and sensitive personal information maintained by the agencies; and
13. Collaborate with federal agencies to protect against, respond to, and recover from cybersecurity incidents.

These responsibilities, powers, and duties are carried out through TXCC's headquarters, the Cybersecurity Threat Intelligence Center, Cybersecurity Incident Response Unit, Digital Forensics Laboratory, Texas Information Sharing and Analysis Organization, Network Security Center (also known as the Network Security Operations Center or NSOC) capability, an online statewide cyber incident reporting portal, a 24-hour cybersecurity hotline, the Cybersecurity Council, Texas Volunteer Incident Response Team (VIRT), and Regional Security Operations Centers (RSOCs), where established.

TXCC executes its mission through law, policy, standards, architecture, agreements, contracts, common services, and coordinated operations. The Command will preserve confidentiality, privilege, privacy, public information protections, procurement controls, and covered entity contract requirements, while delivering statewide cyber defense, cyber operational readiness, and cybersecurity resiliency outcomes. Nothing in this plan is intended to expand TXCC authority beyond statute, rule, agreement, or contract.

As of May 2026, TXCC has a headcount of 48 full-time employees and is actively scaling towards an anticipated workforce of 122 employees plus additional necessary knowledge expert contractors.

This strategic plan describes how TXCC will build and mature the state cybersecurity program during Fiscal Years 2027 to 2031. This plan connects TXCC's statutory mandate to four agency goals: enhancing cybersecurity readiness, strengthening cyber resilience, growing Texas's skilled cybersecurity workforce, and sustaining the administrative functions required to operate the agency.

Vision

TXCC's vision is that the state of Texas is secure in cyberspace, protected by a trained, ready, proactive, effective cybersecurity workforce and strengthened by advanced, resilient cybersecurity capabilities. TXCC will achieve this vision by leading a coordinated statewide security program that turns threat intelligence into protective action, strengthens common standards and services, expands workforce capacity, builds public trust, and protects Texas's data and critical systems within the authorities granted by law.

For this planning period, TXCC's strategic direction is to shift the state's cyber posture from primarily reactive incident response toward proactive prevention, enhanced readiness, and increased resilience. TXCC will prioritize integrated intelligence, early risk identification, scalable standards and services, common operational capabilities, threat-informed protective action, exercises, and workforce development that help stop incidents before they disrupt Texans, public services, or critical infrastructure. This plan positions TXCC to become a premier statewide cyber defense command that turns statutory authority into measurable operational impact. Success should be visible in stronger readiness, faster detection and response, better evidence and reporting, broader workforce capacity, more resilient public services, and clearer statewide coordination across Texas's cyber defense ecosystem.

By Fiscal Year 2031, Texas will be a national model for cyber readiness and resilience: able to prevent avoidable incidents before they occur, detect threats earlier, respond faster, preserve evidence, and restore essential public services and critical infrastructure with confidence. A combination of common procedures, technology acquisition, well-designed architecture, and partnerships will set conditions across the state through operational maneuver in cyberspace to preserve security, maximize availability, and reduce adversary activity and presence.

"Operational maneuver" is a desired feature of TXCC's functional mission design (with a Cybersecurity Threat Intelligence Center (CTIC), Information Sharing and Analysis Organization (ISAO), and a Unified Cyber Task Force (UCTF)) and six operational cyberspace terrains. Successful operational maneuver begins with cyber threat intelligence insights, i.e., knowledge of who the adversary is and how they might be targeting Texas. That knowledge drives daily decision-making about how to secure, protect, and defend Texas's networks across the six operational terrains, not just by TXCC itself, but also by TXCC's stakeholders, partners, and teammates, with whom TXCC is sharing those insights via the ISAO. In short, we are able to deny adversaries access to Texas's cyberspace terrains and, failing that, detect, identify, and eradicate them from Texas's sovereign digital terrain (encompassing information technology, operational technology, critical infrastructure, etc.).

Operational Terrains

TXCC executes its mission to prevent and respond to cyber incidents across six operational cyberspace terrains:

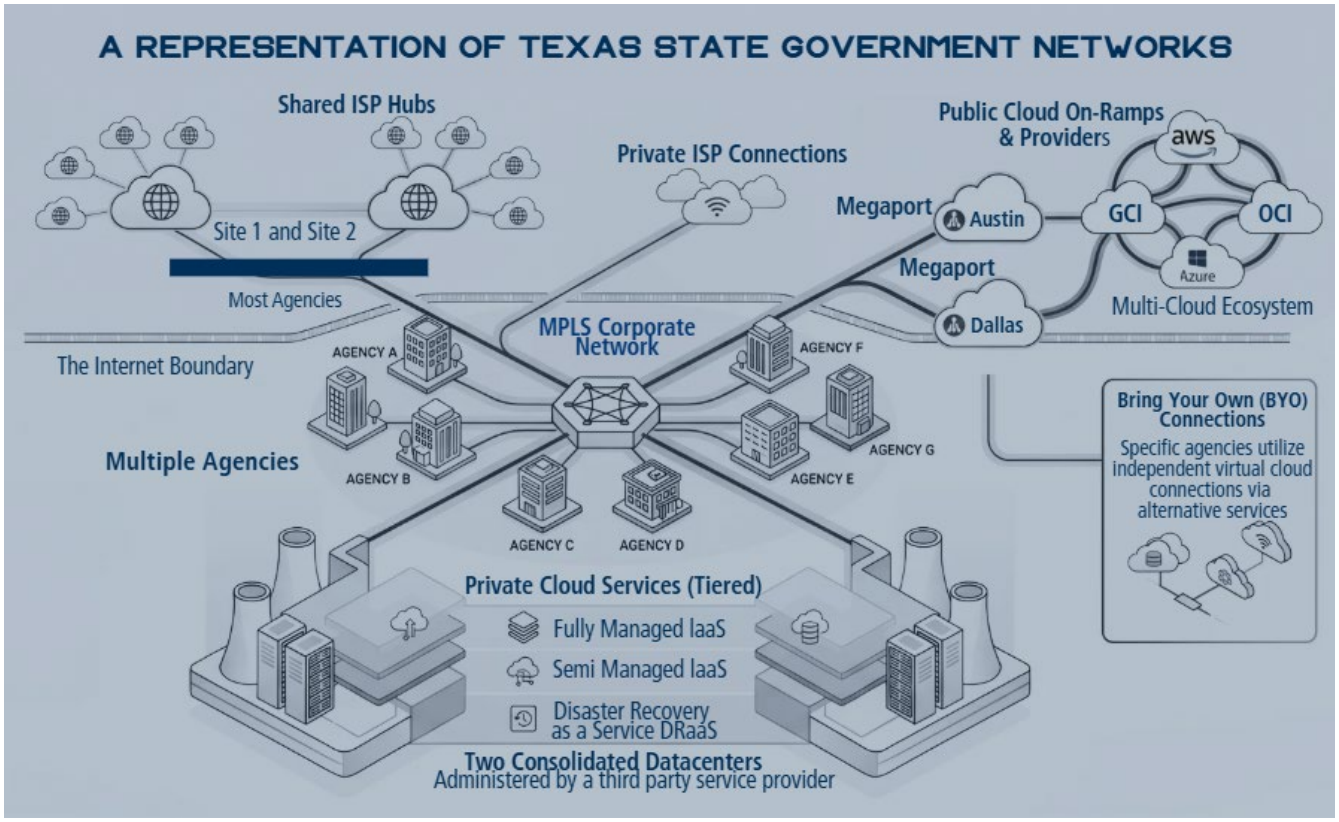
1. Texas state government entities: departments, commissions, boards, offices, or other agencies in the executive branch of state government that was created by the constitution or a statute.
2. Institutions of Higher Education: the university system and institutions of higher education, as defined by Section 61.003, Education Code.
3. Law Enforcement and Judiciary: the supreme court, the court of criminal appeals, a court of appeals, a district court, 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. Texans' data held by the entities listed above.

Texas Government Code Chapter 2063 broadly defines critical infrastructure, including sectors such as chemical, communications, manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation, and water and wastewater systems. It is expected that TXCC will operationalize a cost-recovery model systemically across Operational Terrains 1-4 and will further assess opportunity across Terrains 5 and 6 in the future.

There is substantial complexity in the networks associated with these terrains and therefore in the task of preventing and responding effectively to future cyber incidents. To illustrate the point, the figure below provides a high-level representation of network complexity in Terrain #1 alone (the Texas state

government). It features multiple agencies within a core network backbone, but also agencies outside the core and various agencies with various internet service and cloud service provider arrangements. This graphic captures a snapshot in time whose accuracy will diminish over time.

As of the date of this strategic plan, TXCC has visibility into only a portion of these networks, as reflected by the systems depicted above the dark blue bar. It illustrates the imperative of expanding TXCC's visibility into these networks while also architecting state governments in ways that better prevent cyber incidents, bolster cybersecurity resilience, and enable recovery and restoration of services in the wake of an incident.



Of particular note, as of the date of this strategic plan, is the new pacing threat to networks. The advent of artificial intelligence (AI) models able to identify previously unknown software vulnerabilities (so-called "zero days") and develop exploits at a previously unimaginable pace gives heightened urgency to the task of securing these six operational terrains.

Philosophy

As described in the next section, TXCC's strategic plan encompasses four major goals. These goals drive two essential outcomes for Texas: greater cyber operational readiness and stronger cybersecurity resilience for Texas. By executing its mission through these four goals, Texas will be better prepared to protect and defend its information and operational technology networks, preserve government and critical infrastructure services, and recover from cyber incidents with speed and minimal disruption.

Pillars

TXCC's strategy is organized around five mission pillars: Prevent, Secure, Protect, Defend, and Educate. Together, these pillars establish the framework for building Texas's statewide cyber defense capability and translating statutory responsibility into measurable operational impact.

Prevent

"Prevent" is the organizing principle for TXCC's statewide cyber defense strategy. It is the mission that drives the Command's highest-value contribution to Texas: stopping cyber threats before they disrupt systems, compromise data, or interrupt essential services. TXCC will prioritize integrated intelligence, early risk identification, proactive vulnerability reduction, and targeted investment in capabilities that deny malicious cyber actors the opportunity to operate inside Texas networks. This pillar will be advanced through robust policies, advanced technical solutions, network segmentation, proactive methods and controls, superior tradecraft, and integration of AI into network defenses.

Secure

"Secure" reflects the daily cybersecurity activities across all sectors and professions required to reduce cyber risk across Texas. It requires a posture that is proactive and deliberate. Texas cannot afford to be passive or reactive in the face of a rapidly evolving threat environment. Through this pillar, TXCC, its partners, and stakeholders across the state will work to establish and maintain secure systems, networks,

data environments, and operational practices. Security must be embedded by design, sustained through disciplined execution, and continuously adapted to meet emerging threats.

Protect

"Protect" underpins TXCC's responsibility to help safeguard the systems, data, and services Texans rely on every day. This pillar focuses on limiting exposure, reducing vulnerability, and containing the potential impact of cyber incidents before they escalate into disruption. TXCC will promote strong security controls, resilient infrastructure, responsible data stewardship, and defense-in-depth practices across state government and critical dependencies. This pillar is grounded in a standard-of-care and a duty to warn, ensuring that Texas entities are better positioned to understand risk, implement safeguards, and protect the services that power Texas.

Defend

"Defend" is the coordinated operational response required when malicious activity threatens or compromises Texas systems. It requires TXCC to synchronize actions across the attack surface, support rapid containment, preserve essential services, and enable restoration of normal operations. Whether an event involves probing, unauthorized access, intrusion, breach, or a significant cyberattack, this pillar focuses on decisive action. TXCC will support coordinated response efforts that remove intruder access, restore system integrity, reduce recurring exposure, and return services to normal with speed, precision, and minimal disruption.

Educate

"Educate" builds the human capacity and capability required for sustained cybersecurity readiness and resilience. Cybersecurity depends not only on technology and tools, but on people who understand risk, execute sound practices, and adapt to evolving threats. TXCC will advance cybersecurity excellence across Texas through awareness, training, technical education, exercises, and workforce development. This pillar will support the broader Texas cyber ecosystem by equipping personnel with relevant knowledge, emerging cyber methods, operational tradecraft, and the confidence to act.

Core Values

TXCC is built on the principle that cybersecurity is a shared responsibility among the Command, its partners, and the communities it serves. Texas cannot meet today's cyber threat environment through isolated action or reactive response. It requires a unified culture of readiness, trust, collaboration, and disciplined execution. TXCC will unite the Texas cyber ecosystem around a shared mission of readiness, resilience, and collective defense. Cybersecurity is not something we have. It is something we do every day through proactive risk reduction, coordinated action, timely communication, and synchronized support. The Command brings stakeholders together to apply the best human expertise, technical capabilities, and public-private collaboration to the state's most pressing cyber challenges. TXCC will operate with urgency, accountability, and purpose. The Command will be proactive rather than reactive,

mission-focused in protecting Texas, responsible in its use of public resources, and innovative in every domain necessary to secure, protect, defend, prevent, and educate across Texas cyberspace. Success will be enabled with a risk-aware, vice risk-averse, mindset.

TXCC's five-year strategy establishes the Command as an indispensable force for Texas cyber defense. Through its five mission pillars, Prevent, Secure, Protect, Defend, and Educate, TXCC aims to stop threats before they cause harm, build resilient systems across government and critical infrastructure, limit disruption when incidents occur, respond with speed and precision, and develop the trained cyber workforce Texas needs to sustain long-term resilience. This plan is not simply about building an agency. It is about building the statewide capability Texas needs to protect the systems Texans rely on, preserve continuity of essential services, and lead the way in cyber readiness and resilience.

In support of the agency's mission, vision, and core values, TXCC's Agency Strategic Plan for Fiscal Years 2027 to 2031 includes the following operational goals:

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

Agency Operational Goals and Action Plans

To make progress toward TXCC's core goals of preventing and responding to cybersecurity incidents and the Governor's statewide initiatives, the agency identified the following operational goals:

GOAL A: ENHANCE TEXAS'S CYBERSECURITY READINESS
AGENCY OPERATIONAL GOAL AND ACTION PLAN
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.
SPECIFIC ACTION ITEMS TO ACHIEVE THE GOAL:
• Build out the CTIC, as specified in Government Code 2063 • Build out the ISAO, as specified in Government Code 2063, and ensure all Texas agencies, departments and entities in all six operational terrains can access relevant cybersecurity information • Engage entities in the six operational terrains to baseline existing cybersecurity budgets, practices, technologies, and cybersecurity information sharing, beginning with the most critical entities of Texas's state agencies and departments and Texas's critical infrastructure • Build out the Digital Forensics Laboratory (DFL), as specified in Government Code 2063

- Deliver transformational cybersecurity capabilities, such as cybersecurity threat intelligence support, information sharing and analysis, 24/7 network monitoring, vulnerability scanning, penetration testing, security assessments, and AI-enabled cybersecurity
- Promulgate guidance to Texas agencies and departments on cybersecurity standards and best practices; extend this guidance to all six operational terrains
- Increase the capacity and capability of statewide cybersecurity operations and services to prevent malicious cyber intrusions into state governmental entities and critical infrastructure networks
- Integrate state-of-the-art AI into Texas state cyber defenses to prevent cybersecurity attacks
- Conduct regular exercises, maintain tested incident response/continuity plans, and track actionable metrics (e.g., detection and response times) to drive improvement

HOW THE GOAL SUPPORTS THE GOVERNOR'S FIVE STATEWIDE OBJECTIVES

TXCC's goal to enhance Texas's cybersecurity readiness supports the statewide objectives to:

- Ensure **accountability** to Texas tax and fee payers by fulfilling the mandates in Government Code 2063 to prevent cybersecurity incidents impacting state governmental and critical infrastructure entities and establishing key organizations within TXCC and improving cybersecurity capabilities and capacities
- Improve **efficiency** and cost-effectiveness by focusing on cybersecurity capabilities and capacity that will yield the highest returns on investment across the six operational cyber terrains in Texas
- Help state agencies, local governments, and institutions of higher education **effectively fulfill core functions** by delivering cybersecurity capabilities and capacity that prevent cybersecurity incidents from impacting these entities
- Provide **excellent partner and stakeholder service** by being proactive in delivering new cybersecurity capabilities and capacity that prevent cybersecurity incidents
- Increase **government transparency** by providing clear, timely communication to stakeholders and the public about TXCC's actions

OTHER CONSIDERATIONS RELEVANT TO THE GOAL OR ACTION ITEM

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.

GOAL B: BOOST THE STATE OF TEXAS'S CYBER RESILIENCE

AGENCY OPERATIONAL GOAL AND ACTION PLAN

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

SPECIFIC ACTION ITEMS TO ACHIEVE THE GOAL:

- Expand cyber incident response and recovery capabilities that assist state government and critical infrastructure entities in securing, protecting, and defending their information and operational technology networks and recovering from malicious cyber intrusions
- Expand upon and transform legacy cyber incident response capabilities and assistance previously provided by DIR by integrating new, state-of-the-art technologies, including AI
- Deliver these capabilities and assistance through entities such as the NSOC, RSOCs, the Cyber Incident Response Unit, and the VIRT
- Coordinate with partner agencies to ensure understanding of capabilities and support efficient and effective service delivery

HOW THE GOAL SUPPORTS THE GOVERNOR'S FIVE STATEWIDE OBJECTIVES

TXCC's goal to enhance Texas's cybersecurity readiness supports the statewide objectives to:

- Ensure **accountability** to Texas tax and fee payers by fulfilling the mandates in Government Code 2063 to prevent cybersecurity incidents impacting state governmental and critical infrastructure entities and establishing key organizations within TXCC and improving cybersecurity capabilities and capacities
- Improve **efficiency** and cost-effectiveness by focusing on cybersecurity capabilities and capacity that will yield the highest returns on investment across the six operational cyber terrains in Texas
- Help state agencies, local governments, and institutions of higher education **effectively fulfill core functions** by delivering cybersecurity capabilities and capacity that prevent cybersecurity incidents from impacting these entities
- Provide **excellent partner and stakeholder service** by being proactive in delivering new cybersecurity capabilities and capacity that prevent cybersecurity incidents
- Increase **government transparency** by providing clear, timely communication to stakeholders and the public about TXCC's actions

OTHER CONSIDERATIONS RELEVANT TO THE GOAL OR ACTION ITEM

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.

GOAL C: CATALYZE GROWTH IN TEXAS'S HIGHLY SKILLED CYBERSECURITY WORKFORCE

AGENCY OPERATIONAL GOAL AND ACTION PLAN

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.

SPECIFIC ACTION ITEMS TO ACHIEVE THE GOAL:

- Fulfill the mandate in Texas Government Code Section 2063.003 to facilitate education and training of Texas's future cybersecurity workforce
- Building upon the training and education programs transferred from DIR to TXCC, transform them through new internships, fellowships, outreach, research, cyber innovation challenges, training platform and modalities, and close collaboration with Texas's institutions of higher education

HOW THE GOAL SUPPORTS THE GOVERNOR'S FIVE STATEWIDE OBJECTIVES

TXCC's goal to enhance Texas's cybersecurity readiness supports the statewide objectives to:

- Ensure **accountability** to Texas tax and fee payers by fulfilling the mandates in Government Code 2063 to prevent cybersecurity incidents impacting state governmental and critical infrastructure entities and establishing key organizations within TXCC and improving cybersecurity capabilities and capacities
- Improve **efficiency** and cost-effectiveness by focusing on cybersecurity capabilities and capacity that will yield the highest returns on investment across the six operational cyber terrains in Texas
- Help state agencies, local governments, and institutions of higher education **effectively fulfill core functions** by delivering cybersecurity capabilities and capacity that prevent cybersecurity incidents from impacting these entities
- Provide **excellent partner and stakeholder service** by being proactive in delivering new cybersecurity capabilities and capacity that prevent cybersecurity incidents
- Increase **government transparency** by providing clear, timely communication to stakeholders and the public about TXCC's actions

OTHER CONSIDERATIONS RELEVANT TO THE GOAL OR ACTION ITEM

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.

GOAL D: INDIRECT ADMINISTRATION

AGENCY OPERATIONAL GOAL AND ACTION PLAN

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 TXCC operations and statutory responsibilities.

SPECIFIC ACTION ITEMS TO ACHIEVE THE GOAL:

- Provide central administrative functions for TXCC's headquarters and subordinate entities
- Manage the agency's finances, while ensuring the integrity of the accounting records and maintaining adequate internal controls to safeguard the agency's financial assets and ensure the compliance of our fiduciary responsibility to the people of Texas
- Promote fiscal responsibility by providing assistance and analysis in planning, administering, and monitoring the budget
- Recruit, hire, develop, and retain the highly qualified workforce needed to support the agency's mission
- Provide information-resource functions, including enterprise applications, information security, telecommunication systems, and data and records management
- Advise agency management on legal matters related to agency programs, employment law, government ethics, procurements, grants and contracting, and the Public Information Act.
- Support the agency's program areas in carrying out rule-making functions
- Provide other support services necessary to ensure that program responsibilities are met

HOW THE GOAL SUPPORTS THE GOVERNOR'S FIVE STATEWIDE OBJECTIVES

TXCC's goal to provide for the administration of TXCC supports statewide objectives to:

- Ensure **accountability** to Texas tax and fee payers by fulfilling the mandates in Government Code 2063 to prevent cybersecurity incidents impacting state governmental and critical infrastructure entities and establishing key organizations within TXCC and improving cybersecurity capabilities and capacities
- Improve **efficiency** and cost-effectiveness by focusing on cybersecurity capabilities and capacity that will yield the highest returns on investment across the six operational cyber terrains in Texas

• Help state agencies, local governments, and institutions of higher education **effectively fulfill core functions** by delivering cybersecurity capabilities and capacity that prevent cybersecurity incidents from impacting these entities • Provide **excellent partner and stakeholder service** by being proactive in delivering new cybersecurity capabilities and capacity that prevent cybersecurity incidents • Increase **government transparency** by providing clear, timely communication to stakeholders and the public about TXCC's actions
OTHER CONSIDERATIONS RELEVANT TO THE GOAL OR ACTION ITEM
TXCC will ensure that each person classified as a contract manager is trained and certified in contract management.

Redundancies and Impediments

TXCC recommends the following changes to address services, state statutes, and state rules or regulations that impede TXCC's fulfillment of its mission and merit additional review.

Clarify Training Requirements for State Agencies and Contractors	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Texas Government Code Section 2054.5191
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or ineffective Agency Operations	While DIR will keep AI training and AI guidance for governmental entities, TXCC will incorporate an AI training component related to cybersecurity. Also, the language is different regarding requirements from what was moved into Texas Government Code Section 2063 and what was repealed, or was not repealed, from Texas Government Code Section 2054. Thus, there remains lack of clarity based on the statutory plain language.
Provide Agency Recommendation for Modification or Elimination	Texas Government Code Section 2054.519 was repealed, but the language in 2054.5191 does not reflect that repeal and that cybersecurity training was moved to TXCC. Those changes should align to the overall training requirements in TXCC's current requirements outlined in Texas Government Code Sections 2063.102 and 2063.103 (such as ensuring that all employees, agents, and contractors need to take cybersecurity training and not limit it to people with 25% access or more).

Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	Clarity for the state agencies and contractors who must comply with the law and how.

Ensure Statutory Clarity for Criminal History Record Information	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Texas Government Code Ch. 411.0765(b)(26) and Texas Government Code Ch. 411.1404
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or ineffective Agency Operations	When DIR's authority for cybersecurity transferred to TXCC, half of the authority for access to Criminal History Record Information went to DIR and half went to TXCC. Both DIR and TXCC need the same full authority.
Provide Agency Recommendation for Modification or Elimination	Texas Government Code Ch. 411.0765(b)(26) should say "the Texas Cyber Command" without qualifiers, just like the other state agencies in the list. Also, there should be corresponding language for TXCC that mirrors what DIR retained in Texas Government Code Ch. 411.1404.
Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	Ability for TXCC and DIR to be secure in cyberspace due to proper background checks based on statutory clarity.

Authorize TXCC To Procure Cybersecurity Technology to Address Cybersecurity Risks More Rapidly Than Standard Procurement Processes Allow	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Purchasing authority under Texas Government Code Ch. 2054 and Ch. 2155
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or	Current purchasing statutes, rules, and requirements are not designed for the speed, duration, or operational complexity of modern cybersecurity threats. They do not provide TXCC sufficient flexibility to make timely, mission-critical purchases when risks exceed a short-term emergency but fall below the threshold for a disaster declaration, nor do they reflect

ineffective Agency Operations	TXCC's specialized expertise in determining the capabilities necessary to protect Texas systems and critical infrastructure.
Provide Agency Recommendation for Modification or Elimination	Add language to permit delegation and exclusion from the comptroller's purchasing authority such as the exemption for HHSC under Texas Government Code Section 2155.144 or for the Railroad Commission of Texas under Texas Government Code Section 2155.150. Exemption language under Texas Government Code Ch. 2054 should be addressed as well.
Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	Ability to act with speed and precision when emerging cyber risks outpace the standard procurement process, including urgent geopolitical threats, rapidly evolving vulnerabilities, and long-term cybersecurity risks that demand timely prevention, mitigation, or response.

Clarify Current Responsibilities Related to Prohibited Technology and Covered Applications	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Prohibited Technology and Covered Applications Texas Government Code Ch. 620
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or ineffective Agency Operations	There is no holistic statute addressing both Prohibited Technology and Covered Applications. TXCC is also replacing DIR in its original role in current practice.
Provide Agency Recommendation for Modification or Elimination	Codify, in one holistic statute, the Executive Orders and the Covered Application statutes related to this topic to provide clarity and ensure consistent compliance. Texas Government Code Ch. 620 needs to be updated to replace DIR with TXCC to reflect current practice and responsibilities.
Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	Updating the language would clarify current responsibilities and assist with consistent compliance.

Codify Current Practice and Statutorily Assign Cybersecurity Responsibilities To TXCC	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Texas Government Code Ch. 2054 (such as sections 2054.033, 2054.0335, 2054.060, 2054.068, 2054.069, 2054.155, 2054.5195, etc.)
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or ineffective Agency Operations	There are cybersecurity responsibilities listed under DIR's statutory authority that belong to TXCC. These have been agreed upon by both agencies.
Provide Agency Recommendation for Modification or Elimination	TXCC recommends replacing DIR with TXCC in the relevant statutes and moving those mentioned statutory cybersecurity responsibilities to Texas Government Code Ch. 2063.
Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	This will codify the current practice and assign cybersecurity responsibilities to the cybersecurity agency to ensure clarity and compliance.

Add TXCC To the List of Member Agencies Listed for The Homeland Security Council	
Service, Statute, Rule, Regulation, Program or State Operation (provide specific citation if applicable)	Texas Government Code Section 421.021
Describe why the Service, Statute, Rule or Regulation is resulting in inefficient or ineffective Agency Operations	The current statutory framework does not adequately reflect the operational nexus between homeland security and cybersecurity, nor does it account for the level of interagency coordination and collaboration now required in practice.
Provide Agency Recommendation for Modification or Elimination	We recommend adding TXCC to the list of member agencies listed for the Homeland Security Council.

Describe the Estimated Cost Savings or Other Benefit Associated with Recommended Change	Codifies current practice and ensures a continued relationship between homeland security and cybersecurity.

Supplemental Elements

Schedules A and B: Proposed Budget Structure and Performance Measure Definitions[1]

GOAL A

Enhance Texas's Cybersecurity Readiness

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.

OBJECTIVE 01 (A.01)

Build Out and Elevate Texas Cyber Command's "Prevent" Mission

Increase the capacity and capability of statewide cybersecurity operations and services to prevent malicious cyber intrusions into state governmental entities and critical infrastructure networks.

STRATEGY 01 (A.01.01)

Enable CTIC, ISAO, and DFL with Transformational Capabilities

Build out the CTIC, ISAO, and the DFL as specified in Government Code 2063. Deliver transformational cybersecurity capabilities, such as cybersecurity threat intelligence support, information sharing and analysis, 24/7 network monitoring, vulnerability scanning, penetration testing, security assessments, and AI, to prevent cyber intrusions into state governmental entities and critical infrastructure.

A.01.01 | Output Measure 01 Threat Intelligence Alerts, Advisories, and Recommendations Issued	
Definition	The number of threat intelligence products issued by TXCC, including alerts, advisories, and mitigation recommendations, that provide actionable information on emerging threats, vulnerabilities, and recommended defensive actions to supported entities.
Purpose	Measures the volume and dissemination of actionable threat intelligence to Texas entities. Higher output reflects enhanced situational awareness and supports proactive risk mitigation and informed decision-making across the state.

[1] TXCC's proposed budget structure and performance measure definitions changes are under review by the Legislative Budget Board.

Data Source	TXCC threat intelligence platforms, reporting systems, distribution logs, and analyst records documenting issued alerts, advisories, and mitigation guidance.
Methodology	Count of all threat intelligence alerts, advisories, and mitigation recommendations formally issued during the reporting period. Each distinct product is counted once at the time of dissemination to one or more entities.
Data Limitations	Variability in threat activity may influence output volume. Differences in classification or bundling of intelligence products may affect counts. High volume does not necessarily equate to effectiveness or impact. Distribution tracking depends on consistent documentation practices.
Calculation Method	Cumulative
Key Measure	No
New Measure	Yes
Priority	Medium
Target Attainment	Higher than target

A.01.01 | Efficiency Measure 01 Time to Disseminate Threat Intelligence	
Definition	Average time between when an analyst identifies a credible threat lead and when CTIC delivers a Texas-specific advisory, alert, or mitigation recommendation to supported entities. The clock starts whether the threat came from outside CTIC (partners, vendors, ISAO) or was first spotted inside Texas (CTIC research, RSOC alerts, victim reports).
Purpose	Measures how fast CTIC's full intelligence pipeline runs, from first sign of a threat through to a warning landing in front of the appropriate Texas entities. Drives investment in accelerating time-to-warning and time-to-protection, including collection sources, analyst capacity, and partner relationships.
Data Source	CTIC case management and production tracking systems; ingestion logs from threat intelligence platforms; partner feeds; commercial threat intelligence vendor systems; ISAO inbound channels; DFL case management records; RSOC alert and escalation logs; CTIC hunt operation records; Texas Cybersecurity Hotline incident intake records; TXCC publication and distribution records.
Methodology	For each Texas-specific advisory, alert, or mitigation recommendation issued during the reporting period, the timestamp of CTIC's first ingestion of the originating credible source is compared to the timestamp of delivery to supported entities. Elapsed time is calculated for each response (advisory, alert, mitigation recommendation, etc.) sent to supported entities, and the average is derived across all products issued during the reporting period. For products developed from multiple contributing sources, the earliest contributing source timestamp is used.

Data Limitations	Accurate timing requires consistent logging across all intake channels. Threats CTIC discovers internally, or that Texas victims report directly, may have less precise start times than threats that arrive through federal partner feeds. Some intelligence carries sharing restrictions that delay publication regardless of how fast analysts work. Some products are built from months of observation; their long cycle times reflect the nature of the work, not slow response to urgent threats.
Calculation Method	Sum of (Advisory Delivery Timestamp – First Ingestion Timestamp) ÷ Total number of Texas-specific advisories issued during reporting period
Key Measure	Yes
New Measure	Yes
Priority	Medium
Target Attainment	Lower than target

GOAL B

Boost the State of Texas's Cyber Resilience

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

OBJECTIVE 01 (B.01)
Respond to and Recover from Malicious Cyber Intrusions

Expand cyber incident response and recovery capabilities that assist state government and critical infrastructure entities in securing, protecting, and defending their information and operational technology networks and recovering from malicious cyber intrusions.

STRATEGY 01 (B.01.01)
Transform Cyber Incident Response Capabilities Transferred

Expand upon and transform legacy cyber incident response capabilities and assistance previously provided by DIR through the integration of new, state-of-the-art technologies, including AI. Deliver these capabilities and assistance through entities such as the NSOC, RSOCs, the Cyber Incident Response Unit, and the VIRT. Coordinate with partner agencies to ensure understanding of capabilities and support efficient and effective service delivery.

B.01 | Outcome Measure 01 Change in Cyber Incidents of the Same or Similar Nature	
Definition	The percentage change in repeat cybersecurity incidents among entities that previously received TXCC incident response support or TXCC issues remediation recommendations, where the subsequent incident involves matching a root cause, vulnerability, threat vector, or attack pattern.
Purpose	Measures the effectiveness of remediation, root cause analysis, and sustained defensive improvements. A decrease in repeat incidents indicates improved

	security posture, reduced exploitable weaknesses, and better long-term risk management.
Data Source	TXCC incident response and case management systems, Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) platforms, vulnerability management tools, and reporting from supported entities.
Methodology	Calculated as the percentage of increase or decrease in the number of incidents by categories compared to the previous reporting period. Incidents are classified based on matching root cause, vulnerability, or attack pattern.
Data Limitations	Accurate classification depends on consistent incident categorization and root cause analysis. Variability in reporting across entities may affect comparability. Increased detection capabilities may initially increase identified repeat incidents. Changes in threat landscape may influence recurrence rates.
Calculation Method	Noncumulative
Key Measure	No
New Measure	Yes
Priority	Medium
Target Attainment	Lower than target

B.01 | Outcome Measure 02 **Reduction in Average Time from Compromise to Detection and Mitigation**	
Definition	The average amount of time between initial compromise or threat entry into a system and the point at which the threat is detected and mitigated. Applicable incidents are those in which TXCC has sufficient telemetry, forensic evidence, or case records to estimate compromise time and mitigation time with reasonable confidence.
Purpose	Measures the effectiveness of detection and response capabilities. Shorter times indicate improved visibility, faster detection, and more efficient incident response, reducing the likelihood of operational disruption or data compromise.
Data Source	TXCC security operations platforms, including SIEM, EDR, incident response systems, forensic analysis reports, and threat intelligence tools.
Methodology	Calculated as the average duration (in hours or days) between estimated time of initial compromise and time of mitigation across all applicable incidents during the reporting period. Time of compromise is determined through forensic analysis and available telemetry.
Data Limitations	This is limited to entities covered by the TXCC SOC or RSOC services. Initial compromise time is often estimated and may not be precisely known. Detection gaps, limited logging, or delayed reporting can affect accuracy. More

	advanced threats may evade detection longer, skewing averages. Variability in entity capabilities may impact consistency.
Calculation Method	Noncumulative
Key Measure	Yes
New Measure	Yes
Priority	High
Target Attainment	Lower than target

B.01 | Outcome Measure 03 Percent Change of Agencies' Security Maturity Over Repeat Assessments	
Definition	Calculation of average percentage growth rate in maturity scores for agencies that underwent repeat Texas Cybersecurity Framework (TCF) assessments.
Purpose	This measure will focus on the effectiveness of the TXCC third-party assessments to improve the organization's security maturity. It will also assist in increased awareness of threats to information resources.
Data Source	Data will be obtained from final assessment reports performed by the managed security services vendor.
Methodology	Average percentage change in security maturity scores (level of adherence to the TCF) for all repeat assessments completed. Scores are based on the Capability Maturity Model and range from 0-5 with: • 0 - None, Nonexistent; • 1 - Ad-hoc, Initial; • 2 - Consistent, Repeatable processes; • 3 - Compliant, Defined; • 4 – Risk-based, Managed; • 5 – Efficient, Optimized.
Data Limitations	Number of agencies completing repeat assessments during the quarter. Fluctuation of maturity due to outside circumstances (e.g., change in staff). In addition, not all organizations who receive TXCC-funded assessments will have a previous score.
Calculation Method	Noncumulative
Key Measure	Yes
New Measure	Yes
Priority	High
Target Attainment	Higher than target

B.01.01 | Output Measure 01 Entities Receiving Continuous Diagnostics and Mitigation Services	
Definition	The number of Texas entities that actively receive operational and Continuous Monitoring, Diagnostics, and Mitigation (CDM) capabilities during the reporting period.
Purpose	Measures the expansion of statewide cybersecurity coverage and adoption of centralized security services. Higher onboarding numbers indicate increased visibility, standardized protection, and improved collective defense across Texas entities.
Data Source	TXCC onboarding records, service provisioning systems, platform enrollment data, and executed service agreements with participating RSOC entities.
Methodology	Count of entities that have completed onboarding during the reporting period. Onboarding is considered complete when CDM services are operational and the entity is actively receiving continuous monitoring and threat detection support.
Data Limitations	Onboarding timelines may vary based on entity size, complexity, and resource availability. Partial deployments may not be counted until fully operational. Changes in eligibility or participation may affect totals. Data depends on accurate tracking of onboarding completion.
Calculation Method	Cumulative
Key Measure	Yes
New Measure	Yes
Priority	High
Target Attainment	Higher than target

B.01.01 | Output Measure 02 Coordinated Cyber Defense and Tabletop Exercises Conducted	
Definition	The number of coordinated cybersecurity exercises conducted or supported by TXCC, including operational cyber defense exercises and tabletop exercises, with partner entities. Includes exercises supported by RSOCs.
Purpose	Measures efforts to enhance preparedness, coordination, and incident response capabilities across Texas entities. Exercises improve readiness, validate procedures, and strengthen collaboration among participating organizations.
Data Source	TXCC training and exercise records, RSOC reports, after-action reports, and participation logs documenting conducted exercises.
Methodology	Count of coordinated cyber defense and tabletop exercises conducted during the reporting period. Each exercise is counted once, regardless of the number

	of participating entities. Includes both TXCC-led and TXCC or RSOC-supported exercises.
Data Limitations	Exercise scope and complexity may vary, limiting comparability across events. Participation levels may differ by entity. Informal or internal exercises may not be consistently captured. Volume does not directly measure effectiveness or readiness outcomes.
Calculation Method	Cumulative
Key Measure	No
New Measure	Yes
Priority	Medium
Target Attainment	Higher than target

B.01.01 | Output Measure 03 **Entities with Active RSOC Service Agreements**	
Definition	The number of Texas entities with an executed and active service agreement with a RSOC authorizing the provision of cybersecurity monitoring, detection, and response support services during the reporting period.
Purpose	Measures the expansion of formal cybersecurity service adoption through RSOCs. A higher number reflects increased engagement, standardized service delivery, and broader access to coordinated statewide cyber defense capabilities.
Data Source	Executed RSOC service agreements, TXCC contract management systems, onboarding records, and legal/administrative documentation confirming active client relationships.
Methodology	Count of unique client entities with fully executed and active RSOC service agreements during the reporting period. Each client entity is counted once per active agreement, regardless of service scope or duration within the period.
Data Limitations	Timing of contract execution and onboarding may affect reporting periods. Renewal cycles or amendments may impact counts. Some entities may have a phased or partial service activation not immediately reflected in totals. Data depends on accurate contract tracking and status updates.
Calculation Method	Cumulative
Key Measure	Yes
New Measure	Yes
Priority	High
Target Attainment	Higher than target

B.01.01 | Output Measure 04 Number of Students Participating in RSOC Programs and Activities	
Definition	The number of students who participate in RSOC programs, including internships, apprenticeships, training programs, simulations, exercises, or other structured educational engagements coordinated through TXCC and RSOC partners during the reporting period.
Purpose	Measures the RSOC's role in workforce development and cybersecurity talent pipeline growth. Higher participation reflects expanded educational outreach, skills development opportunities, and strengthened alignment between academic institutions and state cybersecurity operations.
Data Source	RSOC program enrollment records, TXCC workforce development tracking systems, partner institution reports, internship and training attendance logs, and exercise participation rosters.
Methodology	Count of unique students who participate in at least one RSOC-supported program or activity during the reporting period. Each student is counted once per reporting period regardless of multiple engagements.
Data Limitations	Participation data may vary depending on partner reporting practices and program definitions. Students engaged in informal or unstructured activities may not be captured. Duplicate counting is avoided through unique participant tracking but may be affected by inconsistent reporting across entities.
Calculation Method	Cumulative
Key Measure	No
New Measure	Yes
Priority	Medium
Target Attainment	Higher than target

B.01.01 | Output Measure 05 Number of Completed State Security Assessments	
Definition	The number of completed third-party TCF cybersecurity assessments conducted for Texas entities under TXCC-supported security assessment programs during the reporting period.
Purpose	Measures the level of participation in statewide cybersecurity assessment activities and supports identification of agency security capability gaps and recommended risk mitigation actions.
Data Source	TXCC assessment tracking systems, vendor-delivered assessment reports, and TXCC program records documenting completed security assessments and final report issuance.

Methodology	Count of completed security assessments delivered to eligible Texas entities during the reporting period. Each assessment is counted once upon completion and final delivery of assessment findings to the participating entity.
Data Limitations	Scheduling and resource constraints may affect the timing and number of completed assessments within a reporting period.
Calculation Method	Cumulative
Key Measure	Yes
New Measure	Yes
Priority	Medium
Target Attainment	Met target

B.01.01 | Output Measure 06 Number of Completed Penetration Tests	
Definition	The number of completed TXCC-sponsored third-party black box penetration tests conducted on state agency and other authorized Texas entity networks during the reporting period.
Purpose	Measures the extent of proactive network security testing performed to identify vulnerabilities and support remediation efforts that strengthen the cybersecurity posture of Texas entities.
Data Source	TXCC program tracking systems, third-party vendor assessment reports, contract deliverables, and finalized penetration testing reports issued to participating entities.
Methodology	Count of completed penetration tests performed for eligible Texas entities during the reporting period. Each completed engagement is counted once upon delivery of final test results and findings to the participating entity.
Data Limitations	Participation is voluntary and may vary by entity. Scope, depth, and complexity of penetration tests may differ across engagements, limiting comparability. Retesting and phased testing activities may be inconsistently reported if not clearly defined as separate engagements.
Calculation Method	Cumulative
Key Measure	Yes
New Measure	Yes
Priority	Medium
Target Attainment	Met target

B.01.01 | Efficiency Measure 01 Cost per Completed Penetration Test Delivered to Eligible Entities	
Definition	The average cost incurred to deliver a completed black box penetration test conducted for TXCC-supported entities during the reporting period.
Purpose	Measures cost efficiency in delivering standardized cybersecurity assessment services and supports evaluation of resource utilization relative to assessment demand.
Data Source	Vendor invoices, contract expenditure records, and TXCC financial tracking systems documenting penetration testing services delivered.
Methodology	Total cost of black box penetration testing services delivered during the reporting period divided by the total number of completed penetration tests.
Data Limitations	Costs may vary based on scope, complexity, and size of assessed entities. Vendor pricing structures and bundled service offerings may affect comparability across reporting periods. Participation by higher education and public junior college entities is voluntary, which may influence sample size and cost variability.
Calculation Type	Noncumulative
Key Measure	No
New Measure	Yes
Priority	Medium
Target Attainment	Lower than target

GOAL C

Catalyze growth in Texas's highly skilled cybersecurity workforce

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.

OBJECTIVE 01 (C.01)

Facilitate Education and Training of a Future Cybersecurity Workforce

Fulfill the mandate in Texas Government Code Section 2063 to facilitate education and training of a cybersecurity workforce.

STRATEGY 01 (C.01.01)

Transform Training and Education Programs Transferred from DIR to TXCC

Building upon the training and education programs transferred from DIR to TXCC, transform them through new internships, fellowships, outreach, research, cyber innovation challenges, and close collaboration with Texas's institutions of higher education.

C.01.01 | Output Measure 01 Percentage of Entities Participating in Cybersecurity Training	
Definition	Percentage of eligible Texas entities that participate in at least one TXCC-led or TXCC-supported cybersecurity training offering including webinars, conferences, seminars, skills enhancement, or other training offerings related to cybersecurity, during the reporting period.
Purpose	Measures statewide engagement and awareness in cybersecurity preparedness through participation in TXCC-led or TXCC-supported training programs.
Data Source	Training attendance records, registration systems, and virtual and in-person participation logs.
Methodology	Total Organizations Participating in the reporting period divided by Number of Active Organizations multiplied by 100.
Data Limitations	Attendance data may be inaccurate if participants fail to register individually for web-based training or sign in for in-person sessions.
Calculation Method	Noncumulative
Key Measure	Yes
New Measure	Yes
Priority	Medium
Target Attainment	Higher than target

GOAL D

Indirect Administration

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 TXCC operations and statutory responsibilities.

OBJECTIVE 01 (D.01)
Central Administration

STRATEGY 01 (D.01.01)
Central Administration

Schedule C: Historically Underutilized Business Plan

Mission

TXCC will administer the Historically Underutilized Business (HUB) Plan in compliance with all HUB statutory and regulatory requirements.

Overview

As a newly established agency, TXCC is currently reliant on DIR to assist with purchasing and has inherited contracts that transferred from DIR's cybersecurity and network teams. New purchases are made with DIR's assistance, and both agencies are working together to ensure HUB compliance.

Fiscal Year 2026 Goals

TXCC's HUB goals align with the State of Texas HUB utilization goals and procurement categories established by the Texas Comptroller of Public Accounts.

HUB Programs, Processes, And Activities

TXCC complies with all HUB statutory and regulatory requirements. As a new agency, TXCC currently relies on DIR's procurement. Any HUB programs, processes, or activities would be inherited from DIR.

Schedule D: Statewide Capital Planning for Fiscal Years 2028-2029

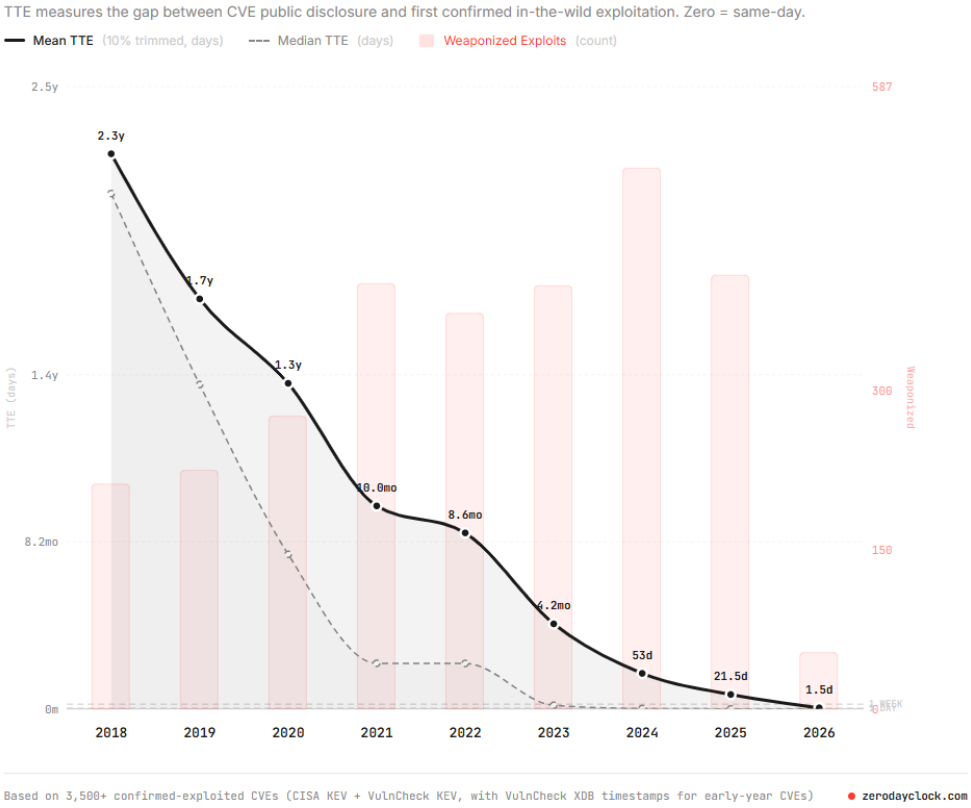
As a new agency, TXCC is continuing to build a capital plan for Fiscal Years 2028-2029. However, as part of TXCC's initial analysis of its mission, the cyber threat landscape impacting the state of Texas, emerging technologies likely to impact cybersecurity in the near term, such as AI, TXCC has identified three areas likely to require capital investment in cybersecurity in the next few years:

- Establishment of statewide, managed cybersecurity services program
- The use of AI to secure existing software stacks, and
- A managed transition to post-quantum encryption in state agency systems and networks.

First, TXCC will continue to assess the capital investments needed to establish a statewide, managed cybersecurity services program that delivers common, scalable, and interoperable security capabilities to state agencies and other authorized entities. This evaluation will define the core shared service baseline required to support the NSOC, RSOCs, threat intelligence integration, shared telemetry, data ingestion, security monitoring, exposure management, case management, and coordinated response. It may also evaluate the need for managed firewall services, endpoint and network detection and response, SIEM capabilities, expanded threat intelligence platform services, statewide commercial threat intelligence licensing, incident collaboration tools, service management functions, and related integration, identity, data protection, and operational support requirements.

The latest AI models, such as Anthropic's Claude Mythos, represent a massive leap forward in cyber capabilities and are fundamentally reshaping the cyber threat landscape around the world. Large Language Models being developed by other AI companies are now able to identify software vulnerabilities at a previously unimaginable scale. As shown in the graphic below, these models enable nation-state adversaries and criminals to reduce the time between the discovery of a previously unknown vulnerability (a so-called "zero-day" vulnerability) and the exploitation of that vulnerability to a day or less.

From Vulnerability to Exploitation



In the hands of adversary nation-states and cyber criminals, these models can identify software vulnerabilities and the exploits to take advantage of these vulnerabilities leading to unauthorized intrusions in government and private sector networks. Texas will be impacted by these developments.

Second, TXCC will evaluate the capital investments needed to prepare Texas for the speed, scale, and complexity of cybersecurity in an AI-enabled threat environment. This planning area is not limited to internal agency adoption of AI. The evaluation will examine how AI can be used to identify and remedy current and emerging vulnerabilities across state government and critical infrastructure networks, as well as to counter adversary use of AI for cyber reconnaissance, phishing, malware development, social engineering, and campaign execution. It may assess opportunities for AI-assisted detection and triage, automated enrichment, threat intelligence correlation, analyst decision support, cyber risk analytics, AI system security guidance, adversarial AI monitoring, model and data protection requirements, governance controls, validation methods, and training needed to help Texas entities operate securely as AI accelerates the tempo of cyber offense and defense.

Third, the emergence of quantum computers, on a timeline that remains uncertain, will fundamentally reshape the cybersecurity landscape by rendering today's internet encryption methods vulnerable to exploitation by adversaries and criminals. TXCC will assess the capital investments required to help state agencies transition to quantum-resistant cryptography. This planning effort includes identifying where

current cryptographic systems, certificates, keys, protocols, applications, identity systems, cloud services, network services, and vendor solutions may be susceptible to future quantum risk. The evaluation may include risk prioritization, migration planning, public-key infrastructure modernization, certificate lifecycle management, post-quantum cryptography pilots, procurement guidance, vendor readiness assessments, and implementation support to state agencies with high value data, long-term confidentiality needs, or critical service dependencies.

As TXCC grows its statewide cyber defense, the Command will require a dedicated facility that supports secure operations, specialized technical work, workforce growth, and long-term mission execution. This capital planning effort will include space for the DFL and other mission-critical functions.

Over the next two years, TXCC will determine what investments it recommends for closing existing gaps in statewide cybersecurity capabilities and for addressing emerging technologies that are poised to reshape the cybersecurity ecosystem in profound ways. The goal is to strengthen Texas's cyber operational readiness and position Texas to prevent cybersecurity incidents at a scale previously not achievable with existing technology. By aligning personnel, technology, secure workspaces, and operational capabilities in one integrated environment, TXCC will establish the physical foundation necessary to scale operations, sustain readiness, and deliver the cyber defense capabilities Texas requires.

Schedule F: Workforce Plan

Part I: Agency Overview

TXCC is building an operationally focused organization that advances two overarching strategic outcomes: increased cyber operational readiness and strengthened cybersecurity resiliency for the State of Texas, as outlined in Section 1.

As of May 2026, TXCC has 48 personnel on board. Thirty-two individuals were transferred from DIR. TXCC has hired 16 directly. TXCC plans to add an additional thirty-six personnel to its roster by the end of FY26 and an additional 38 personnel by the end of FY27. The planned hiring program will bring TXCC's total personnel complement to 122 personnel.

TXCC has compiled initial estimates of the personnel it requires to fulfill the functions specified in Texas Government Code 2063, including staffing the CTIC, Information Sharing and Analysis Organization, the elements comprising the UCTF, which includes the NSOC, Cybersecurity Incident Response Unit (CIRU), and DFL, and headquarters.
If TXCC receives the full personnel complement identified in its initial requirements estimate, the Command's total workforce would reach approximately 180 personnel.

CRITICAL WORKFORCE SKILLS

The mission of TXCC requires a workforce that possesses advanced cybersecurity expertise and strong partnership and collaboration instincts. Success depends on a balanced mix of technical proficiency spanning fields such as information and operational technology, cyber physical systems, and adversary threat intelligence, and mission-aligned soft skills. Together, a workforce with these attributes ensures TXCC can enhance cyber operational readiness, strengthen cybersecurity resiliency, and facilitate cybersecurity education and training. Workforce headcount and skills are critical to the agency's ability to operate. To operate effectively, TXCC's workforce must have the following skills in:

Technical & Job-Specific Skills

- Cyber threat intelligence & analysis
- Cyber threat hunting
- Vulnerability management and risk assessment
- Attack surface management
- Network architectures and network enumeration
- Network and end-point cybersecurity
- Cloud security
- Identity authentication and management
- Artificial intelligence
- Security engineering
- Data science, architectures, analysis, and visualization
- Incident response
- Digital forensics and investigations
- Cyber operations management
- Resiliency and risk management
- Cybersecurity project and program management
- Industry and academic outreach
- Procurement
- State of Texas fiscal management
- Statutory compliance

General Professional Skills

- Organizational leadership
- Critical thinking and problem solving
- Partner and stakeholder and engagement
- Cross-organizational collaboration
- Consensus building
- Change management
- Clear, concise communications
- Ethical judgement and decision-making

Part II: Workforce Analysis

CURRENT TXCC WORKFORCE

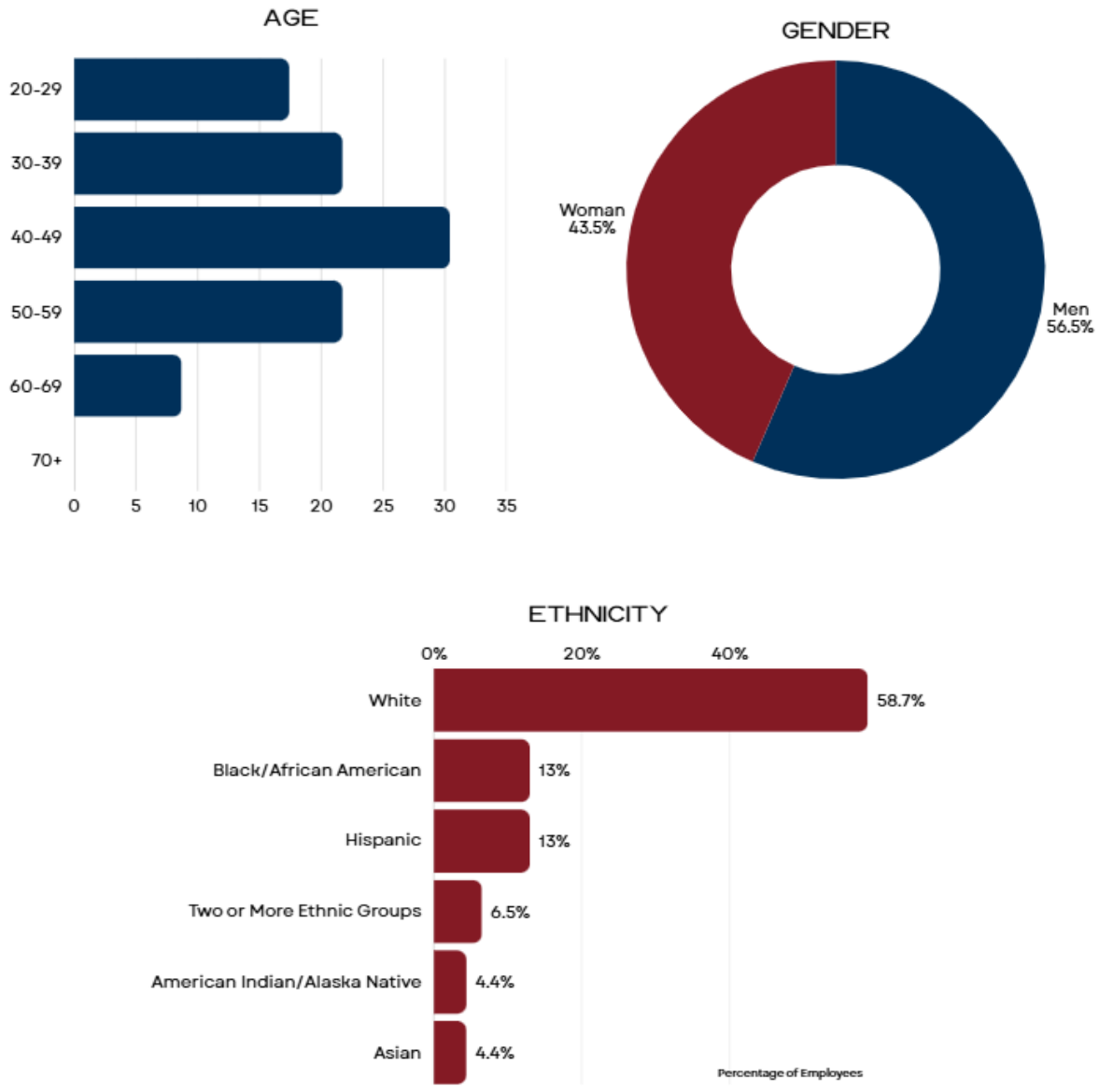
As a newly established agency, TXCC is in the early stages of building and assessing its workforce. As of May 2026, TXCC has a headcount of 48 full-time employees and is actively scaling toward an anticipated workforce of 122 employees, with a headquarters located in San Antonio and operational elements in San Antonio and other locations.

This section provides a baseline profile of the current workforce, including demographics, workforce allocation, and retirement eligibility. Although data on turnover and engagement and exit surveys are not yet available, this analysis establishes a foundation for future workforce planning and decision-making.

DEMOGRAPHICS

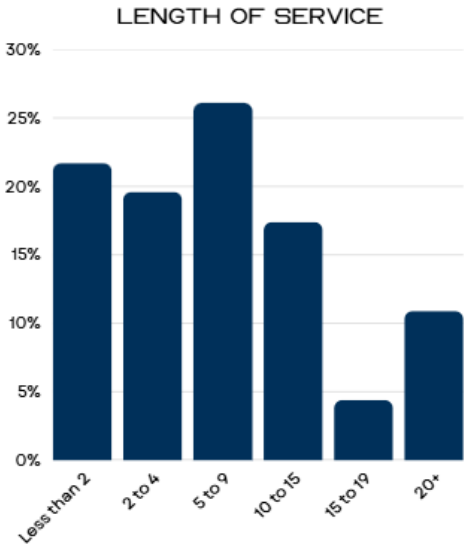
Age

The age distribution of the TXCC workforce reflects a balanced mix of early-career, mid-career, and experienced professionals. The largest segment of employees falls within the 40–49 age range (30%). Twenty-two percent of the workforce is aged 30-39, and another 22% are aged 50-59. Smaller proportions of employees in the 20–29 (17%) and 60–69 (8.7%) ranges further support a multi-generational workforce poised for knowledge transfer and long-term sustainability.



Length of State Service

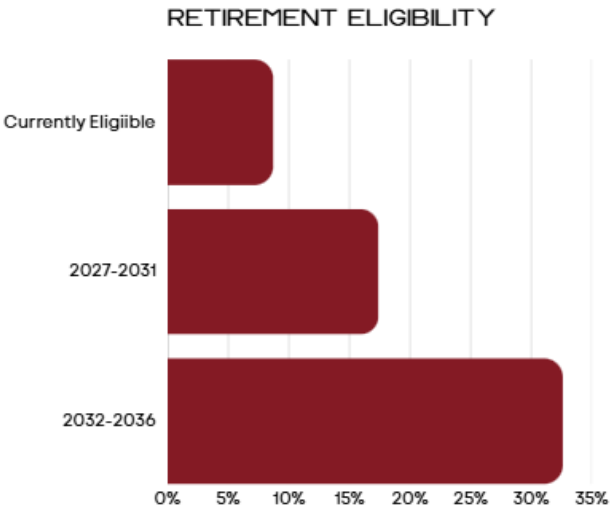
The TXCC workforce encompasses a strong concentration of mid-career employees, with 26% of the workforce having 5–9 years of service to the state. Employees with less than 5 years of service constitute 41% of the workforce, while 33% of the workforce have 10 or more years of experience and therefore provides additional depth and institutional knowledge. This balance supports both immediate operational capability and continued workforce development as the agency grows.



RETIREMENT FORECAST

In the near term, retirement eligibility within the TXCC workforce is relatively limited but increases steadily over time. Currently, four employees (8.7%) of the workforce are eligible to retire, while an additional 8 employees (17%) are projected to be retirement-eligible within the next five fiscal years. Fifteen employees (33%) will be within the next ten fiscal years. TXCC also employs one return-to-work retiree, reflecting early efforts to leverage experienced talent.

These projections, based on ERS retirement criteria and individual service factors, indicate a growing need for succession planning and knowledge transfer strategies as the agency matures.



MILITARY EMPLOYMENT

TXCC is committed to leveraging the skills and experience of service members, veterans, and eligible family members through the military employment preference. Currently, individuals receiving military employment preference make up 26% of the workforce (12 employees), exceeding the State of Texas goal of at least 20%. TXCC is well-positioned to attract and integrate this talent pool into mission-critical operations as the agency grows.

TURNOVER

Due to the agency's recent formation and ongoing workforce build-out, there is no historical data available to assess turnover trends. As TXCC continues to grow and mature, turnover metrics will be monitored and analyzed to inform future workforce planning and retention strategies.

ENGAGEMENT & EXIT SURVEYS

As a newly established agency, TXCC has not yet conducted employee engagement or exit surveys. As TXCC continues to grow, these tools will be implemented to gather insights that inform employee experience, retention, and organizational effectiveness strategies.

Demand Analysis – Future TXCC Workforce

EXTERNAL FACTORS IMPACTING TXCC

TXCC's future workforce needs will be shaped by a highly competitive cybersecurity labor market. Cybersecurity skills are in high demand in the private sector. This demand will continue to increase. Cyber threats targeting government, critical infrastructure, education, and public-sector partners continue to increase and accelerate. Agentic AI and other technology developments have the potential to greatly expand our vulnerabilities in cyberspace.

Nationally, the U.S. Bureau of Labor Statistics projects employment for information security analysts to grow 29% from 2024 to 2034, significantly faster than the average for all occupations. This trend will exert continued pressure on recruitment and retention of cybersecurity talent.[2] In 2025, Texas employed more than 103,000 cybersecurity workers while nearly 40,000 cybersecurity jobs remained unfilled.[3] This data reinforces TXCC's competition with private industry, federal partners, higher education, and other public entities for the same specialized talent pool. It also illuminates the breadth and depth of technical and mission expertise required to be a good-faith cybersecurity partner across Texas's economy and sector stakeholders.

---

[2] U.S. Bureau of Labor Statistics. (2024). *Information security analysts*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[3] CyberSeek. (n.d.). Cybersecurity supply-and-demand heat map. https://www.cyberseek.org/heatmap.html

The agency's workforce will also be affected by the expanding scope and complexity of cyber threats. For example, the federal Director of National Intelligence evaluates cyberspace as a growing strategic threat, with state-backed actors from China, Russia, Iran, and North Korea leading campaigns against U.S. infrastructure and networks. Adversaries increasingly employ advanced digital technologies to achieve military, economic, and political advantages. Ransomware remains one of the most significant threats to public-sector and critical infrastructure organizations.[4] The FBI reported more than 3,600 ransomware complaints nationally in 2025[5], while Verizon's 2025 public-sector analysis found ransomware present in 30% of public-sector data breaches.[6] These trends will require TXCC to maintain strong capabilities in threat intelligence, vulnerability management, incident response, digital forensics, continuity planning, and interagency coordination.

Emerging technologies will further shape TXCC's staffing and training needs. AI, automation, cloud services, identity and access management, and data analytics are now core technology issues for state leaders.[7] The National Association of State Chief Information Officers' priorities identified cybersecurity and risk management, AI, data management, legacy modernization, identity and access management, cloud services, and workforce among the top priorities for state governments.[8] TXCC will need a workforce that can broaden its skills quickly and integrate new tools responsibly in cybersecurity operations and enterprise support functions.

Finally, the agency's readiness will depend not only on cyber operation personnel, but also on the operational-enabling workforce required to sustain a new state agency. The U.S. Department of Commerce's National Institute of Standard and Technology elevated "Govern"[9] as a core cybersecurity function, emphasizing that cybersecurity risk management policy, strategy, expectations, and oversight must be established, communicated, and monitored.[10] For TXCC, this means human resources, legal,

---

[4] World Economic Forum. (2025). Global cybersecurity outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[5] Federal Bureau of Investigation. (2025). Internet Crime Report 2025. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[6] Verizon. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[7] Gartner. (2026). Gartner identifies the top cybersecurity trends for 2026. https://www.gartner.com/en/newsroom/press-releases/2026-02-05-gartner-identifies-the-top-cybersecurity-trends-for-2026

[8] National Association of State Chief Information Officers. (2024). State CIO top 10 priorities for 2025. https://www.nascio.org/wp-content/uploads/2024/12/NASCIO-2025-State-CIO-Top-10-Priorities.pdf

[9] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[10] National Institute of Standards and Technology. (2024). Post quantum cryptography standards. https://www.nist.gov

procurement, finance, records management, project management, communications, and executive administration skills will be essential to mission execution, regulatory compliance, vendor oversight, workforce development, and long-term organizational resilience.

FUTURE SKILLS & CRITICAL FUNCTIONS

As TXCC continues to scale its workforce, the agency remains equally committed to integrating emerging technologies into cybersecurity operations in ways that enhance mission execution and effectiveness. TXCC's culture is built on being "future-ready," ensuring the organization can pivot quickly, adopt innovative tools, and stay ahead of an evolving, thinking adversary.

LABOR MARKET COMPETITION

For a newly established agency like TXCC, several structural and market-driven factors may limit its competitiveness in attracting and retaining talent. This is especially true in a high-demand field like cybersecurity. The key factors impacting TXCC's labor market competitiveness include:

- Competition for Specialized Skill Sets – There is a national shortage of cybersecurity talent, and TXCC must compete with private sector employers, federal agencies, contractors, and higher education institutions for the same limited pool of highly skilled candidates.
- Compensation Gaps with Private Sector – Cybersecurity professionals often earn significantly higher salaries in private industry, particularly in areas like cloud security, threat intelligence, and AI. State compensation structures, while stable, may not always keep pace with market rates. State job classification systems can also limit flexibility in setting salaries, offering incentives, or rapidly adjusting roles to meet evolving cybersecurity needs.
- Lengthy Hiring Processes – State government hiring processes can be more time-intensive compared to positions in the private-sector. This can result in losing candidates to faster-moving employers.
- Workplace Flexibility Expectations – Many cybersecurity professionals expect fully remote or highly flexible work environments. State policies, security requirements, and/or operational needs may limit the degree of flexibility TXCC can offer.
- Limited Brand Recognition – As a newly formed organization, TXCC does not yet have the established reputation or visibility that attracts candidates organically, particularly compared to well-known tech companies or federal agencies.
- Training and Experience Gaps in the Labor Pool – Entry-level pipelines may not always produce candidates with the hands-on experience required for immediate operational roles, requiring additional investment in training and development.
- Geographic Considerations – While San Antonio has a growing cybersecurity presence, competition within the region with military, federal, and private employers can exacerbate hiring challenges. Additionally, employees with skills and experience using state technologies, like Centralized Accounting and Payroll/Personnel System, are often located in and around Austin.

ANTICIPATED FTE DEMAND

Based on current mission scope, operational requirements, and industry benchmarks for cybersecurity organizations, TXCC anticipates a fully operational workforce once the agency meets its appropriate FTE limit. However, examining the future cybersecurity landscape in Texas, TXCC will likely have the workload capacity to support approximately 180 personnel. This estimate reflects the staffing required to support 24/7 cyber operations, statewide coordination demands, and the integrated operational support functions necessary to sustain a matrixed command structure.

Gap Analysis

RESOURCE SHORTAGES & SURPLUSES

As TXCC continues to build toward its anticipated full operational capacity, current staffing levels reflect a resource shortage relative to projected needs. With 48 filled positions and a near-term growth target of 122 employees, the agency is still in a scale-up phase and has not yet reached the staffing levels required to fully support all mission areas across the six operational terrains. The most significant shortages exist in specialized cybersecurity roles, 24/7 operational coverage, integration with DPS fusion center and TDEM state operations center, and key operational support functions necessary to sustain a matrixed command structure. A fully mature TXCC will be measured against its ability to generate state-wide cyber operational readiness and cybersecurity resiliency with agility, speed, mass, and scale.

At this stage, there are no identified workforce surpluses as all existing positions are aligned to immediate operational priorities and organizational build-out. As the agency matures, ongoing evaluation will be necessary to ensure resources remain balanced across mission execution, governance, and support functions.

SKILL SHORTAGES & SURPLUSES

TXCC currently faces skill shortages in several high-demand and emerging areas, particularly in advanced cybersecurity disciplines such as threat intelligence, cloud security, incident response, and security engineering. Additionally, there is a growing need for skills related to AI, automation, and data analytics to support a more proactive and scalable cybersecurity posture. Beyond technical capabilities, there is also demand for experienced professionals in governance, risk management, compliance, and enterprise-level program management to support statewide coordination and oversight responsibilities.

No significant surplus of skills has been identified at this time. TXCC is intentionally building a workforce with wide-ranging and complementary skill sets. Continued investment in training, cross-functional development, and workforce planning will be critical to closing identified gaps and maintaining alignment with evolving mission requirements. In parallel, TXCC will deliberately pursue a partnership with TMD to find every opportunity to align mission with capacity and capability.

RISKS DERIVED FROM WORKFORCE SHORTAGES

Workforce shortages present several risks to TXCC's ability to fully execute its mission. Insufficient staffing may limit the agency's ability to provide services across all operational terrains, especially in the near term. Shortages in specialized skill areas could also delay the implementation of key initiatives related to emerging technologies, risk management, and statewide coordination.

External factors, including strong competition for cybersecurity talent, compensation limitations, and hiring timelines, elevate these risks. Addressing these challenges will require strategic workforce planning, targeted recruitment, and continued investment in employee development to ensure TXCC can scale effectively and maintain operational readiness.

Part III: Workforce Strategies

OVERVIEW

To address identified workforce gaps and support continued growth, TXCC will implement targeted strategies across workforce sourcing, recruitment, development, and organizational change management. These strategies are designed to build a sustainable, future-ready workforce capable of meeting evolving mission demands and long-term operational effectiveness.

RECRUITMENT STRATEGIES

Workforce & Recruitment Sourcing

TXCC will implement a multi-channel workforce sourcing and recruitment strategy designed to attract and sustain a high-caliber, mission-driven workforce across both cybersecurity and operational support functions. As the agency continues to scale, TXCC remains committed to integrating emerging technologies into cybersecurity operations in ways that strengthen its ability to recruit talent with future-focused skill sets. The agency will build strong talent pipelines through partnerships with Texas universities, community colleges, military transition programs, and professional networks, while also leveraging military employment preference programs and state workforce mobility to attract experienced candidates.

TXCC's culture is built on being "future-ready," enabling the organization to pivot quickly, embrace new tools, and remain at the forefront of mission effectiveness. To support this, the agency will engage with learning and professional development organizations to implement workforce programs that promote continuous learning, adaptability, and culture change. Recruitment efforts will be complemented by the development of apprenticeship and internship programs, alongside the active pursuit of top-tier industry talent to fulfill immediate staffing needs and long-term workforce sustainability.

To remain competitive, TXCC will focus on reducing time-to-hire, strengthening employer brand recognition, and clearly communicating opportunities for purpose, impact, and professional growth. The agency recognizes that retention begins with a culture of mutual respect, where employees are

encouraged to contribute ideas, provide feedback, and shape the organization's future. By fostering innovation and empowering its workforce, TXCC aims to build a dynamic organization that is indispensable to the State of Texas.

WORKFORCE DEVELOPMENT

Ship Programs

TXCC will implement a comprehensive suite of "Ship Programs" to build sustainable talent pipelines and support long-term workforce development. These programs are designed to strengthen early-career pathways, expand access to cybersecurity careers, and reinforce TXCC's commitment to being a future-ready organization that invests in continuous learning and community engagement.

Traditional Internships

- TXCC will partner with Texas colleges, universities, and certification programs to establish a robust and flexible internship program, including micro-internships, summer internships, and course-integrated experiences. These opportunities will provide hands-on exposure to cybersecurity and operational support functions, creating a pipeline of future employees while also expanding cybersecurity awareness across the state. Even when interns do not transition directly into TXCC roles, they will be valuable partners and advocates in their future careers.

SkillBridge Internship Program

- TXCC will participate in the Department of Defense SkillBridge program to provide internships and training opportunities for transitioning service members. This program enables the agency to attract highly skilled, mission-oriented talent with experience in complex and high-security environments, while supporting service members as they transition into civilian careers.

Apprenticeship Programs

- TXCC will explore and develop apprenticeship programs in collaboration with local educational institutions, particularly in the Austin and San Antonio regions. Building successful models implemented by other state agencies, these programs will provide structured, earn-while-you-learn pathways for developing talent in cybersecurity and related fields, helping to address workforce shortages while creating accessible entry points into state service.

Mentorship (Internal) Program

- TXCC will establish an internal mentorship program to support employee development, knowledge transfer, and career progression. This program will connect employees across departments and experience levels, fostering collaboration and strengthening the agency's matrixed command structure.

Mentorship (External) Program

- TXCC will expand mentorship opportunities beyond the agency by partnering with local schools, colleges, and universities. Through these efforts, the Command will engage with students and emerging professionals to promote cybersecurity careers, build relationships with future talent, and support the development of the broader cybersecurity workforce in Texas.

Together, these Ship programs will serve as a cornerstone of TXCC's workforce development strategy, ensuring a steady pipeline of skilled talent while reinforcing a culture of learning, adaptability, and mission-driven growth.

Learning & Development

TXCC is committed to fostering a culture of continuous learning to ensure its workforce remains adaptable, skilled, and mission-ready in a rapidly evolving cybersecurity landscape. TXCC will invest in ongoing professional development opportunities, including technical training, leadership development, certifications, and cross-functional learning, to strengthen both cyber operations and mission-support capabilities.

In alignment with its "future-ready" culture, the agency will partner with learning and development organizations to deliver training that enhances agility, supports emerging technologies, and promotes innovation. By encouraging employees to expand their skills and knowledge, TXCC will build a resilient workforce capable of meeting current demands while preparing for future challenges.

TXCC is committed to recognizing and reinforcing a Texas Cyber Workforce cohort that can be leveraged to support state readiness and resiliency objectives. Drawing from across state and private sectors, organized around RSOCs and the VIRT, this TCWF will grow into a professional community of interest that could be mobilized to support a wide range of state requirements. Underpinning this cohort will be a training and skills assessment platform that could extend from middle school through higher education to government agencies/departments and covered entity stakeholders.

Succession Planning

As the agency continues to scale, TXCC will take a proactive and strategic approach to succession planning to support long-term mission success and workforce sustainability. This includes aligning workforce competencies with the agency's evolving mission and operational needs, while identifying and preparing employees to step into critical roles as the organization grows and matures.

TXCC will implement structured talent development initiatives to support this effort, including individual development plans, expanded mentorship opportunities, and internal mobility pathways that encourage career progression across both cybersecurity and operational support functions. Through ongoing skills assessments and targeted development programs, the agency will strengthen its leadership pipeline, ensure continuity of operations, and position itself as an indispensable partner to the State of Texas.

CHANGE MANAGEMENT

As a rapidly growing organization, TXCC recognizes that effective change management is critical to sustaining momentum and ensuring long-term success. TXCC will adopt a structured, yet flexible approach to managing change, enabling the agency to respond quickly to emerging threats, evolving technologies, and shifting operational priorities while minimizing disruption to mission execution.

The agency will emphasize leadership alignment, clear communication, and employee engagement throughout periods of change, ensuring staff understand the purpose, impact, and benefits of organizational initiatives. By fostering a culture that values adaptability, innovation, and continuous improvement, TXCC will empower employees to embrace change, contribute ideas, and support the agency's ongoing evolution as a future-ready cybersecurity organization.

Part IV: Summary

This workforce plan is based on the agency's strategic plan and considers the organization's mission, vision, and strategic goals. TXCC's workforce plan establishes a strong foundation for building and sustaining a mission-ready workforce capable of protecting the State of Texas in an increasingly complex cyber environment. TXCC has made significant progress in developing its initial workforce requirements and identifying key gaps in staffing levels, specialized skills, and long-term capacity. Through a comprehensive analysis of current workforce composition, future demand, and external labor market factors, the agency is positioned to scale its workforce to meet operational needs across all mission areas and operational terrains.

Schedule G: Workforce Development System Strategic Planning

Not applicable to this agency.

Schedule H: Report on Customer Service

TXCC was established in 2025 to prevent and respond to cybersecurity incidents affecting government entities and critical infrastructure in Texas. In carrying out this mission, TXCC aims to increase Texas's cybersecurity readiness and resiliency. TXCC advances these goals by delivering operational services and support to cybersecurity stakeholders, partners, and teammates, rather than to customers in the traditional sense of the term, such as citizens, businesses, license holders, as contemplated in Texas Government Code Chapter 2114.

As specified in Texas Government Code 2063, TXCC's stakeholders and partners include:

- 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.
- Institutions of Higher Education: the university system and institutions of higher education, as defined by Section 61.003, Education Code.
- Law Enforcement and Judiciary: the supreme court, the court of criminal appeals, a court of appeals, a district court, the Texas Judicial Council, and other agencies in the judicial branch of state government.
- Covered Entities: private entities operating in critical infrastructure or a local government with which TXCC contracts to provide cybersecurity services.

- 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.

Although TXCC provides operational services and support to stakeholders, partners, and teammates across Texas, its engagement model is not transactional. The Command's mission requires trusted, sustained relationships that drive action, improve readiness, and produce measurable cybersecurity outcomes.

TXCC will use a new external engagement framework that reflects a deliberate shift from legacy service-delivery models to an integrated statewide cyber defense ecosystem. Under this framework, stakeholders receive timely insights, advisories, and guidance from the Command and are expected to use that information to reduce risk, strengthen preparedness, and improve operational resilience. Partners engage with TXCC through collaborative, two-way exchanges of data, information, analysis, and action. These relationships enable shared situational awareness, coordinated problem-solving, and faster implementation of cybersecurity practices across sectors. Teammates operate within TXCC's closest mission network. They help shape cyber architectures, operational standards, best practices, and coordinated response capabilities that produce more secure networks and stronger cybersecurity resilience across Texas. TXCC's teammates include, among others, the RSOCs and the VIRT established under Texas Government Code Chapter 2063.

TXCC's goal is to bring stakeholders, partners, and teammates together into a statewide cybersecurity alliance focused on shared readiness, collective defense, and reducing cyber risk. This approach moves beyond traditional customer service. TXCC's work requires proactive engagement, trusted relationships, and ongoing collaboration with agencies, local governments, critical infrastructure operators, education partners, private-sector leaders, RSOCs, and other cyber partners. Through this model, every engagement should help Texas prevent, secure, protect, defend, and educate against cyber threats.

In addition to its broader engagement framework, TXCC will use the cost-recovery authority in Texas Government Code Section 2063.005 to recover the costs of direct technical assistance, cybersecurity training, and other services provided to covered entities. This authority allows TXCC to deliver specialized support beyond baseline services, preserve public resources, and scale assistance when demand exceeds available capacity. To date, TXCC has not yet exercised this authority. As TXCC provides services under a cost-recovery model, the Command will set clear expectations and deliver with accountability, responsiveness, and the level of service quality appropriate for direct operational support.

Schedule I: Certification of Compliance with Cybersecurity Training

CERTIFICATE

Texas Cyber Command

Pursuant to Government Code, Section 2056.002(b)(12), this is to certify that the agency has complied with the cybersecurity training required pursuant to the Texas Government Code, Sections 2063.103 and 2063.104.

Signature

TJWhite
Printed Name

VADM/USN (ret), Chief of Texas Cyber Command
Title

May 31, 2026
Date

Schedule J: Certification of Compliance with Artificial Intelligence Training

CERTIFICATE

Texas Cyber Command

Pursuant to Government Code, Section 2056.002(b)(12), this is to certify that the agency has complied with the artificial intelligence training required pursuant to the Texas Government Code, Sections 2063.103 and 2063.104.

Signature

TJWhite
Printed Name

VADM/USN (ret), Chief of Texas Cyber Command
Title

May 31, 2026
Date

Schedule K: Report on Projects and Acquisitions Financed by Certain Fund Sources

Not applicable to this agency.

Acronym List

AI – Artificial Intelligence
CDM – Continuous Monitoring, Diagnostics, and Mitigation
CIRU – Cybersecurity Incident Response Unit
CTIC – Cybersecurity Threat Intelligence Center
DFL – Digital Forensics Laboratory
DIR – Department of Information Resources
EDR – Endpoint Detection and Response
HUB – Historically Underutilized Business
ISAO – Information Sharing and Analysis Organization
IT – Information Technology
NSOC - Network Security Center (aka Network Security Operations Center)
RSOC – Regional Security Operations Center
SIEM – Security Information and Event Management
TCF – Texas Cybersecurity Framework
TXCC – Texas Cyber Command
UCTF – Unified Cyber Task Force
VIRT – Volunteer Incident Response Team