TXCC
TEXAS CYBER COMMAND

2026 Cybersecurity Report



TEXAS CYBER COMMAND

NOVEMBER 15 2026

Table of Contents

Texas Cyber Command Statement 3
Introduction 5
Concerning Trends in Texas's Cybersecurity Landscape 6
Resource Assessment 9
TXCC Resources 14
Other Government Resources 26
Existing Cybersecurity Statutes Review 26
Legislative Recommendations 27
Preventive and Recovery Efforts 32
Conclusion 36
Appendices 37

NOTE: In this report, the terms "cybersecurity event" and "cybersecurity incident" are not used interchangeably. A cybersecurity incident is a subset of the broader category of cybersecurity events. The National Institute of Standards and Technology defines a cybersecurity event as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). References to statutory cybersecurity incident in this report follow the definition provided in Texas Government Code § 2063.001(6). When presenting operational measures, detections, reported incidents, and confirmed compromises are identified separately to distinguish between observed activity, reported events, and verified impacts.

In this report, the term "state agency" is generally used to indicate a state agency or a state institution of higher education as defined by Texas Government Code § 2063.001 (13), unless otherwise stated.

In this report, the term "technology" is used to indicate information and communications technologies.

Texas Cyber Command Statement

On behalf of Texas Cyber Command (TXCC), I submit the 2026 Cybersecurity Report pursuant to Texas Government Code § 2063.301(a). This biennial report assesses the state's cybersecurity posture and identifies preventive and recovery efforts to strengthen it.

Texas's economic security, essential services, and public safety depend on digital systems that must remain secure and operational. Those systems support emergency communications, deliver power and water, keep classrooms operating, and connect Texans to government services. When they are compromised, the consequences reach far beyond a computer network. Protecting them is essential to protecting Texas.

Cybersecurity incidents are disrupting emergency communications and education, while compromises involving external service providers threaten Texans' personal information. TXCC is leading a deliberate shift from reacting to incidents toward anticipating threats, reducing exposure, and preventing disruption.

Submitted eight months after TXCC's activation, this first Cybersecurity Report assesses available resources, identifies gaps in readiness, and recommends legislative and operational actions to strengthen protection across Texas.

Five converging trends define the challenge:

- **First, digital dependence magnifies the consequences of disruption.** Government services, critical infrastructure, and Texas's economy rely on interconnected systems. A compromise in one environment can affect the organizations and communities that depend on it.
- **Second, cybersecurity readiness varies sharply across Texas.** Smaller jurisdictions and rural communities often lack the staffing, resources, and specialized expertise available to larger organizations, some of which are also under-resourced or have limited and outdated capabilities. These gaps leave essential services exposed and require solutions that reach beyond major population centers.
- **Third, ransomware attacks and data theft continue to grow and impose real costs.** They interrupt services, expose sensitive information, and force organizations to divert resources toward recovery. The burden and impact falls on the Texans who depend on those services.
- **Fourth, emerging technologies are changing the pace of risk**. Artificial intelligence is accelerating the discovery and exploitation of vulnerabilities. Advances in AI-enabled cryptanalysis and quantum computing could undermine widely used encryption, requiring preparation now to protect sensitive information over time.
- **Finally, nation-states and other threat actors are expanding their capabilities.** Their operations are becoming faster, more sophisticated, and more consequential. Geopolitical tensions abroad heighten risks to essential systems here in Texas.

Together, these forces create what TXCC calls "cyber convergence": the intersection of digital dependence, critical gaps in cybersecurity preparedness, and increasingly sophisticated threats. Texas's defenses must keep pace.

Agency survey findings reinforce the need for stronger readiness: only 53 percent of respondents reported adequate budgeted resources for cybersecurity incidents, and 35 percent reported no formal schedule for exercising incident response plans. These self-reported findings underscore the need to test readiness and verify that protective measures and recovery capabilities perform as intended.

TXCC is building a coordinated statewide defense that connects security monitoring, threat intelligence, incident response, digital forensics, and information sharing with regional expertise. As of September 2026, Regional Security Operations Centers (RSOCs) reported preventive services reaching at least 1,975 public entities across 248 counties while developing the cybersecurity workforce. Project Watershed 250 is designed to bring federal, state, local, and private industry capabilities together to strengthen water and wastewater cybersecurity and test a model for broader critical infrastructure protection.

The legislative recommendations in this report advance a clear vision: a Texas that leads the nation in cyber readiness, where Texans are safe in the digital world and essential services remain secure. Six recommendations build on priorities established in TXCC's Agency Strategic Plan for Fiscal Years 2027–2031. Together with additional recommendations from TXCC and members of the Texas Cybersecurity Council, the proposals:

- **Enable earlier protective action** through targeted acquisition authority, shared cybersecurity capabilities, and broader deployment of volunteer expertise.
- **Strengthen operational readiness and accountability** through enforceable minimum standards, recurring exercises, timely access to security data, and clear incident response authority.
- **Expand access to protection** by aligning service eligibility, expanding regional service delivery through RSOCs, and supporting secure critical infrastructure information sharing.
- **Clarify responsibilities and sustain services** by reconciling statutory duties, training requirements, and funding and billing mechanisms following the transfer of cybersecurity functions to TXCC.

Together, these recommendations would remove operational barriers and equip TXCC to deliver coordinated, cost-effective protection at the speed cybersecurity risks demand.

Delivering these capabilities requires sustained invested commitment. TXCC's FY 2028–2029 Legislative Appropriations Request seeks funding to sustain transferred cybersecurity services, add full-time equivalent positions, expand regional service delivery through RSOCs, and address emerging AI and quantum-related risks. The sustainment request would replace historical cost-recovery funding with General Revenue. These requests distinguish the resources needed to sustain existing services from investments needed to expand protection and fulfill the mission the Legislature has assigned.

The Legislature has established the foundation for a stronger cyber defense. Our responsibility is to turn that foundation into dependable protection for Texans. With continued legislative partnership, TXCC is committed to making prevention the standard and sustaining the essential services that keep Texas running.

Thank you for your continued support of TXCC's mission. I am available to brief you or your staff on this report or any related matter.

In abiding service,



Timothy J. White
Vice Admiral, United States Navy (Retired)
Chief, Texas Cyber Command

Enclosure: 2026 Cybersecurity Report

Introduction

Texas Government Code § 2063.301(a) requires the Texas Cyber Command (TXCC) to submit to Texas's leadership by no later than November 15 of each even-numbered year a report that identifies the preventive and recovery efforts the state can undertake to improve cybersecurity. The report must include the following elements:

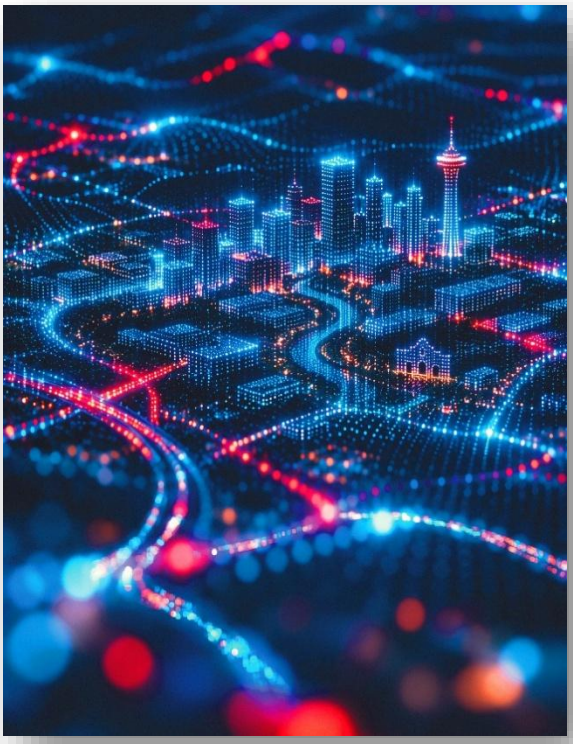
1. An assessment of the resources available to address the operational and financial impacts of a cybersecurity incident;
2. A review of existing statutes regarding cybersecurity and information resources technologies; and
3. Recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity incident.

TXCC submits the 2026 Cybersecurity Report to satisfy this requirement. In this report, TXCC presents data derived from analysis of state agency responses to the Information Resources Deployment Review (IRDR) for Fiscal Year (FY) 2026. The IRDR is the Texas Department of Information Resources (DIR) biennial survey through which state agencies and institutions of higher education report technology deployments, compliance with information-resources statutes and standards, and information technology inventories. The IRDR report is intended to help the Texas Legislature and TXCC assess the state's cybersecurity posture, evaluate the adequacy of existing cybersecurity statutes, and identify legislative changes to strengthen statewide cybersecurity.

The survey data describes agency-reported conditions and are not independent validations of operational effectiveness. DIR received 76 responses from state agencies for each of the 2026 questions in the IRDR, which addressed staffing, incident response resources and plans, and exercise findings. Differences in respondent populations and question wording should be considered when interpreting changes between survey cycles.

TXCC plans to re-examine the IRDR survey design in advance of the FY 2028 review to strengthen the quality and fidelity of cybersecurity posture information gathered in the surveys.

Concerning Trends in Texas's Cybersecurity Landscape

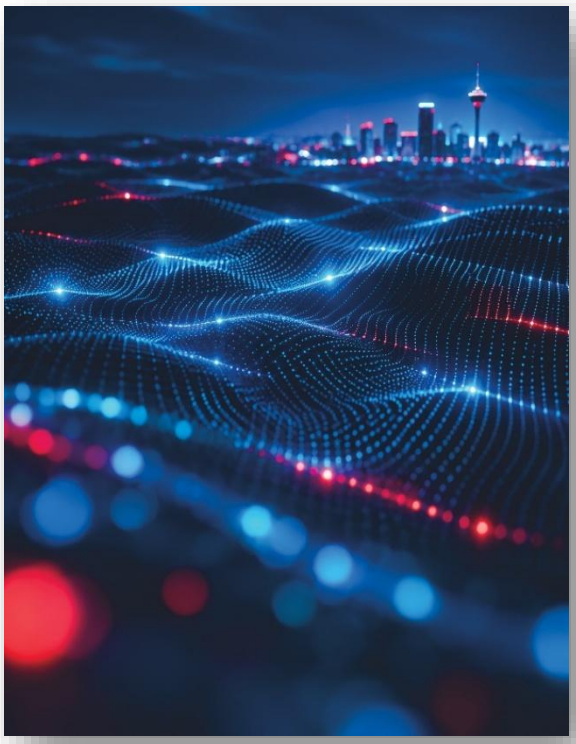


As the eighth-largest economy in the world, a global leader in energy production, and home to critical military installations and major transportation hubs, Texas is critical to the United States's economic prosperity and national defense. Those same attributes make the state an attractive target for malicious cyber actors.

Broadly speaking, Texas is being targeted by three categories of malicious cyber actors and advanced persistent threats. These are:

1. **Nation-state actors**. Known as Advanced Persistent Threats, nation-state actors like China, Iran, Democratic People's Republic of Korea, and Russia, employ sophisticated tradecraft, tactics, techniques, and technology infrastructure. These adversaries tend to emphasize establishing persistent footholds in the networks that they target. These networks are frequently in critical infrastructure sectors such as water, power, transportation, and telecommunications as well as defense-adjacent infrastructure. Volt Typhoon and Salt Typhoon are two examples of People's Republic of China linked groups that have been detected intruding into critical infrastructure inside the United States. It is not known whether nation-state adversaries currently have footholds in Texas state government or critical infrastructure networks. The objective design of the TXCC Cybersecurity Threat Intelligence Center (CTIC) is to discover, assess, and inform prevention against adversary footholds.
2. **Ransomware groups and affiliated criminal entities**. These entities control and encrypt other entities' networks and data, as well as exfiltrate sensitive data from those networks. Encryption renders the networks and data unusable until the entities pay a ransom to regain control of their network, or they rebuild from a known baseline. Victims may also have to pay a ransom to prevent their data from being exposed on the internet. Ransomware groups often target health care systems, local governments, and school districts because they recognize these entities are under pressure to restore services quickly and are therefore often inclined to pay the ransoms. Generating awareness and educating citizens and enterprises across Texas is a design objective of the TXCC Information Sharing and Analysis Organization (ISAO).

3. **Criminals engaged in data theft and exposure**. These actors typically seek to harvest personally identifiable information held by government and commercial entities on citizens and customers to sell the information on the dark web. That information is useful to other criminals who use it for identity theft and fraud. Strengthening a preventive cybersecurity posture across Texas state government networks and around Texans' data held in those networks by Texas state agencies is a design objective of the TXCC Unified Cyber Task Force (UCTF). Prioritizing structure and solutions here facilitate adoption across networks supporting institutions of higher education, law enforcement and the judiciary, covered entities, and critical infrastructure.



Texas faces five converging trends that threaten essential services, economic stability, and Texans' safety in the digital world. Together, they create what TXCC calls "cyber convergence": the intersection of digital dependence, critical gaps in cybersecurity preparedness, and increasingly sophisticated threats.

First, Texas relies on interconnected digital systems and internet connectivity to deliver government services and operate critical infrastructure, including power and water. This connectivity supports nearly every sector of Texas's economy and helps fuel its growth. It also creates dependencies that can magnify the consequences of cybersecurity incidents, making a strong cybersecurity posture essential to sustaining services and economic stability.

Second, Texas's size and differences in local resources create significant disparities in cybersecurity readiness. Large metropolitan jurisdictions may have dedicated cybersecurity teams, established security programs, and access to specialized tools and expertise. Smaller cities, counties, and rural communities often operate with limited IT staffing and budgets while balancing competing priorities. These differences create gaps in the ability to prevent, detect, respond to, and recover from incidents. Strengthening cybersecurity statewide requires approaches that address these resource and capability gaps.

Third, ransomware and data theft continue to threaten Texas organizations. These incidents can interrupt services, expose sensitive information, and impose substantial recovery costs. Their effects extend beyond the affected organization to the residents, businesses, and communities that depend on its services.

Fourth, artificial intelligence (AI) is a dynamic and disruptive cybersecurity challenge. Advances in AI can accelerate the discovery of previously unknown software vulnerabilities and the development of methods to exploit them, increasing the urgency of securing TXCC's six operational terrains: state government entities, institutions of higher education, law enforcement and the judiciary, covered entities, critical infrastructure, and the data held by all of the previously named Texas entities. This shift demands faster detection, continuous assessment, and timely protective action. Advances in quantum computing could also undermine widely used encryption, requiring preparation now to protect sensitive information over the long term.



Finally, nation-states and other threat actors are expanding the speed, scale, and sophistication of their operations. Texas's defenses must keep pace as AI shortens the time available to identify and address vulnerabilities. Geopolitical tensions abroad can heighten risks within Texas, including efforts to disrupt essential services, compromise critical infrastructure, and undermine public trust. This cyber convergence places the systems that support Texans' daily lives at risk, making prevention, readiness, and coordinated defense essential to the state's security.

Examples of Disruptive Cybersecurity Incidents

The following incidents illustrate operational disruption and data risk affecting Texas public services.

In June 2026, a regional 9-1-1 network operator experienced a cybersecurity incident that temporarily disrupted computer systems and public safety applications. During the response and recovery phase, the systems dispatchers rely on to answer and route emergency calls was degraded and manual work arounds had to be implemented during the extended recovery processes.

In August 2026, a Texas institution of higher education experienced a significant cybersecurity incident that disrupted core educational systems as the fall semester began. The incident's speed and complexity hindered the university's ability to maintain normal operations during a critical period for students, faculty, and staff and contributed to an extended recovery process. The disruption underscores the importance of early threat detection, tested continuity plans, and coordinated incident response to sustain educational services and restore essential systems.

Disruptive security incidents continue to affect government entities and private sector partners across Texas, disrupting service delivery, causing financial loss, and eroding trust among those affected.

A Case Study in Data Theft

As noted in Texas Parks and Wildlife Department's (TPWD) public notice, TXCC detected a cybersecurity incident involving the department's hunting and fishing license service provider on May 13, 2026. The investigation indicated that an unauthorized party may have obtained customer contact information, driver's license information, and passport numbers associated with more than three million license customers. TPWD reported that Social Security numbers, birth dates, and financial information were not obtained.

The incident underscores the need to assess and manage cybersecurity risks across both agency-operated systems and services operated by third parties. Securing an agency's internal environment alone does not ensure the protection of government data held or processed by external service providers.

Resource Assessment

This section of the report contains an assessment of the resources available to address the operational and financial impacts of a cybersecurity incident.

State Agency Resources

Texas's state government comprises more than 150 state agencies. On top of that, there are thousands of local government entities across the state. Together, these entities are an attractive target for cyber threat actors due to the sheer number of public-sector information assets that house sensitive and confidential information. Compounding the issue, state agencies must balance competing priorities with limited IT resources, which makes preventing and responding to cybersecurity incidents a challenge.

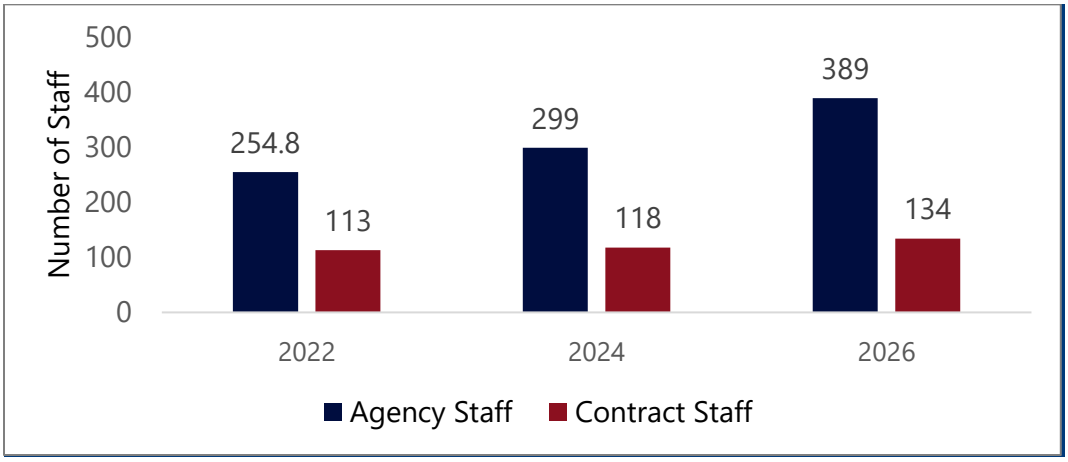
State Agency Cybersecurity Resources

State law requires the Texas Department of Information Resources (DIR) to conduct the Information Resources Deployment Review (IRDR), a biennial survey through which state agencies and institutions of higher education report technology deployments, compliance with information-resources statutes and standards, and information technology inventories. Texas Government Code § 2054.1211 exempts institutions of higher education from reporting the results of their IRDR to DIR except to the extent that DIR requires it by rule.

This year's survey results indicate that agencies prioritized cybersecurity in alignment with the 2026 – 2030 State Strategic Plan for Information Resources Management.

Figure 1 presents reported agency security staffing and contractor positions from the 2022, 2024, and 2026 surveys. The 2026 responses identify 389 currently employed dedicated agency security professionals and 134 contractor positions expected over the next biennium. These measures have different time bases and should not be interpreted as a single current workforce count.

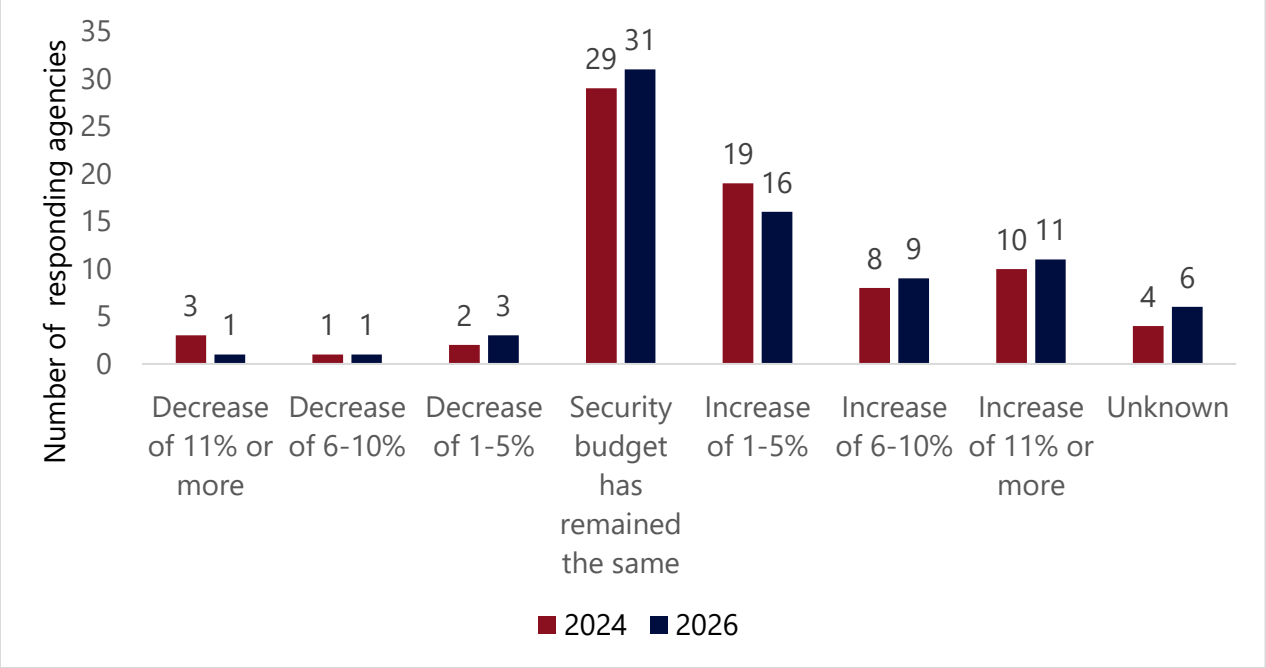
Figure 1 | Reported Agency Security Staffing and Contractor Positions, 2022, 2024, and 2026 Surveys



Source: 2026 Information Resources Deployment Review

Figure 2 compares agencies' reported biennial security-budget trends in the 2024 and 2026 surveys.

Figure 2 | Reported Biennial Trend in Agency Security Budgets, 2024 and 2026 Surveys



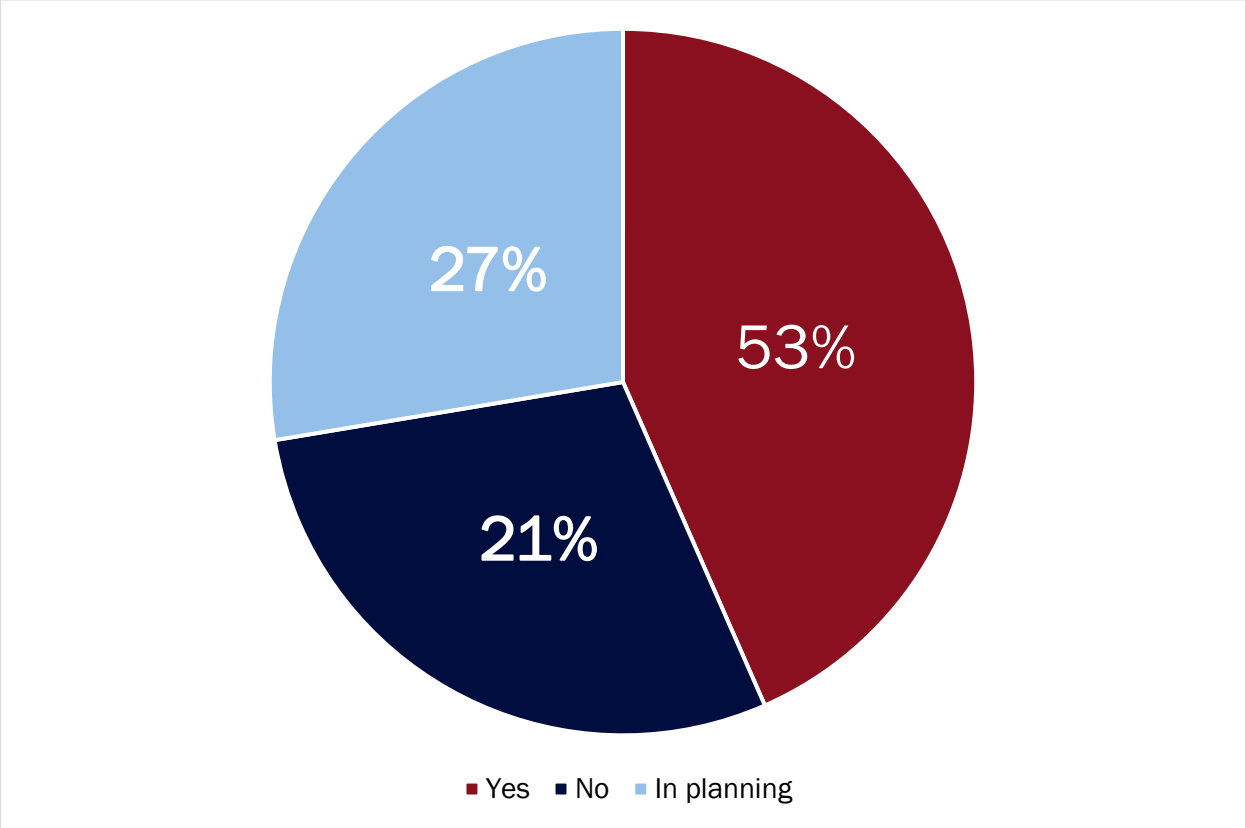
Source: 2026 Information Resources Deployment Review. Responses: 76 in 2024 and 78 in 2026

State Agency Cybersecurity Incident Response

Figure 3 presents agencies' reported adequacy of budgeted resources for cybersecurity incidents. Among 78 respondents, 41 agencies (53%) reported adequate resources, 16 (21%) reported that they did not, and 21 (27%) reported resources in planning. Planned resources are reported separately from resources identified as currently adequate.

TXCC and other public- and private-sector resources can support incident response, but available assistance should not be treated as a substitute for each entity's own preparedness, recovery planning, and resource requirements. Incident response capability is necessary but insufficient to defeat the threat, dependency, and vulnerability confronting Texas.

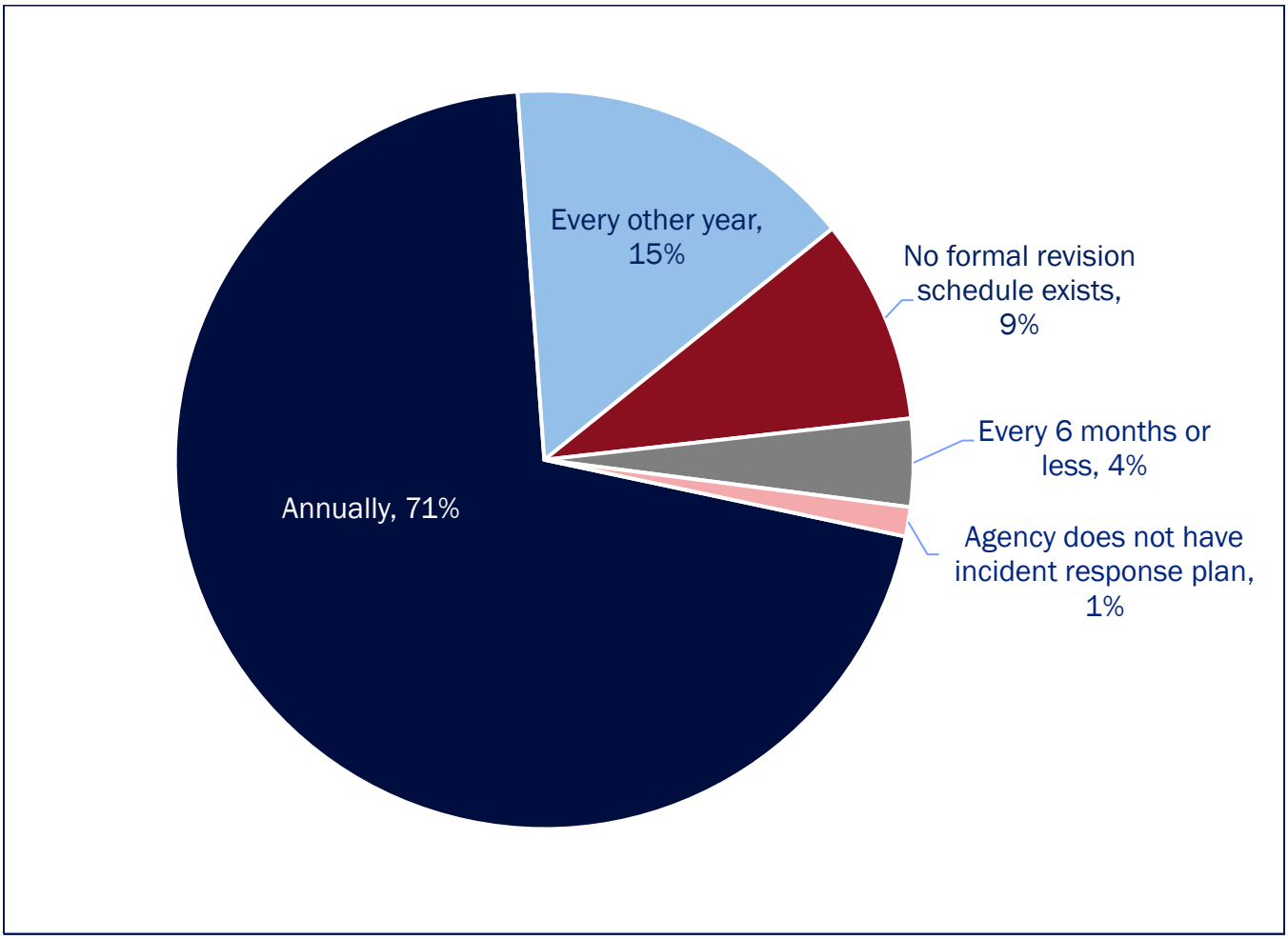
Figure 3 | Percent of State Agencies Who Report Having Adequate Resources Budgeted for Cybersecurity Incidents



Source: 2026 Information Resources Deployment Review; 78 responses.

Incident response planning and review activities can reduce the overall incident costs associated with potential compromises. The United States Cybersecurity and Infrastructure Security Agency (CISA) recommends entities review their incident response plan at least quarterly. Although three respondents (4%) reported in 2026 that they review their incident response plans every six months or less, as shown in Figure 4, this response category does not establish how many agencies review their plans at least quarterly.

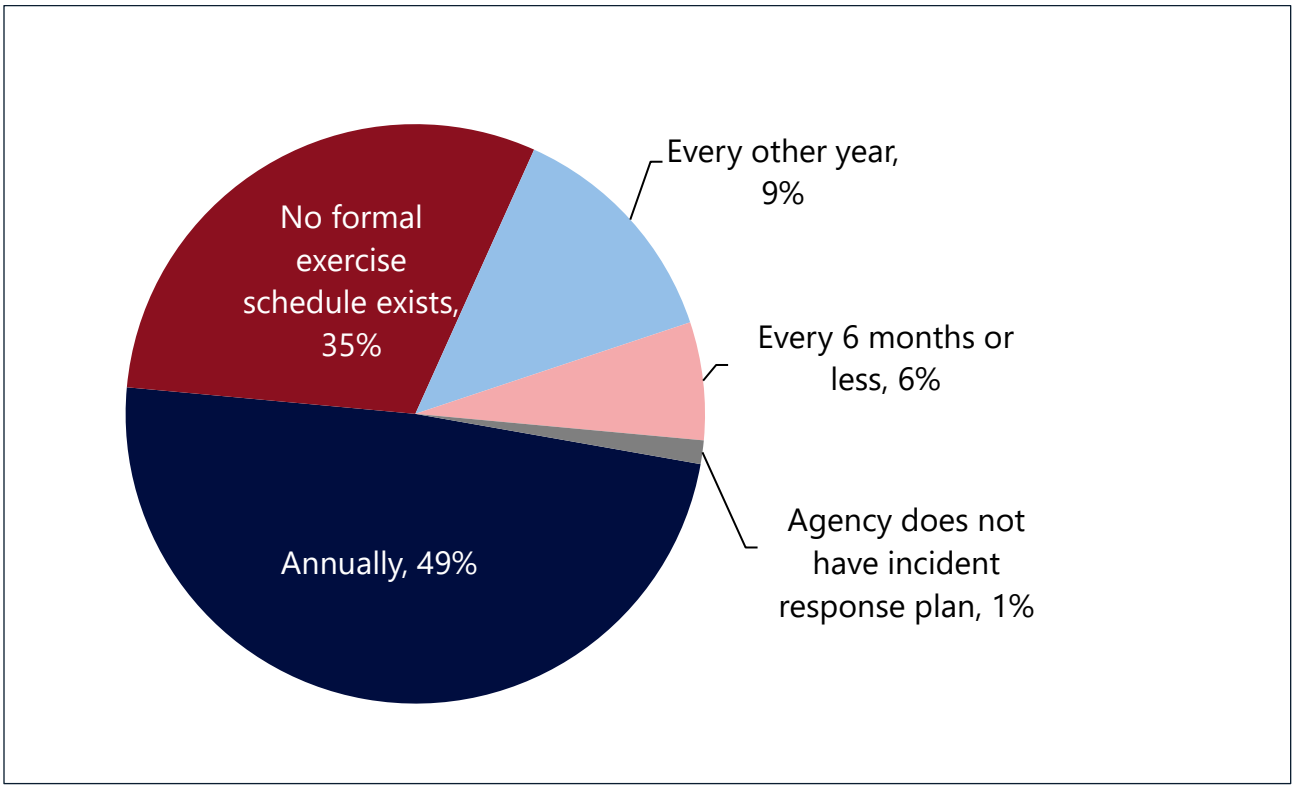
Figure 4 | Frequency at Which State Agencies Review Cybersecurity Incident Response Plans



Source: 2026 Information Resources Deployment Review; 78 responses.

As shown above in Figure 4, 55 state agencies (71%) reported annual plan reviews, 12 (15%) reported reviews every other year, and seven (9%) reported no formal revision schedule in 2026. However, incident response plan reviews and incident response exercises are separate readiness activities. Figure 5 separately presents the frequency of incident response exercises. Of the 78 respondents, 38 (49%) reported annual incident response exercises, while 27 (35%) reported no formal exercise schedule. Seven (9%) reported exercises every other year, five (6%) reported exercises every six months or less, and one (1%) reported having no incident response plan.

Figure 5 | Frequency at Which State Agencies Report Exercising Cyber Incident Response Plans



Source: 2026 Information Resources Deployment Review; 78 responses.

State Agency Resources Assessment Summary

The survey findings describe reported staffing, budget trends, incident-resource adequacy, and preparedness practices. Increased staffing or spending does not by itself establish that incident-response resources are adequate. Plan maintenance and incident response exercises are separate readiness activities, and the survey's six-month-or-less review category does not establish quarterly review frequency. These results should inform priorities for staffing, preparedness, and recovery capacity, while remaining distinct from independently validated operational performance.

TXCC Resources

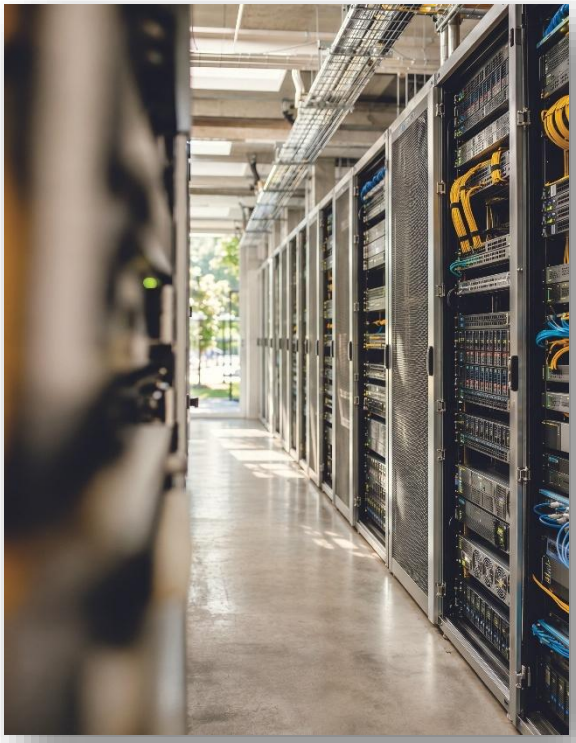
TXCC provides state agencies with access to cybersecurity resources through multiple programs. This section provides an overview of the major cybersecurity resources provided by TXCC. TXCC's operating model connects shared security monitoring and technical services with incident response, digital forensics, regional service delivery, and threat intelligence.

The Information Sharing and Analysis Organization is a statewide information-sharing and partner-engagement organization. The Unified Cyber Task Force integrates the Security Operations Center, the Cybersecurity Incident Response Unit, and the Digital Forensics Lab operations. The Cybersecurity Threat Intelligence Center provides intelligence analysis and guidance, while the Information Sharing and Analysis Organization supports information sharing and partner engagement. The Regional Security Operations Centers provide regional delivery and workforce development.

This TXCC model is intended to turn findings from individual incidents into broader protection for participating entities and establish an increased preventive posture across the state.

Unified Cyber Task Force

TXCC has established the Unified Cyber Task Force (UCTF) as the operational arm for securing, defending, and recovering Texas networks. The UCTF unites three capabilities under one coordinated structure: the Security Operations Center (SOC), the Cybersecurity Incident Response Unit (CIRU), and the Digital Forensics Laboratory (DFL).



Security Operations Center

In accordance with Texas Government Code § 2059.101 and § 2059.104, TXCC operates SOC to provide cybersecurity monitoring and protection for participating state agencies and connected environments. Its work includes perimeter defense, distributed denial-of-service mitigation, endpoint security, phishing analysis, and alerting. The SOC coordinates incident response with the CIRU and draws on the DFL and Cybersecurity Threat Intelligence Center (CTIC) for forensic and intelligence support.

TXCC is expanding this capability through a common security operations environment that connects state agency services with regional service delivery. Work includes continued implementation and integration of the shared Security Information and Event Management (SIEM) environment, broader asset and vulnerability visibility, and automated defensive workflows. CTIC supplies threat intelligence to inform detection, investigation, and protective action; RSOCs contribute regional operations and partner coordination.

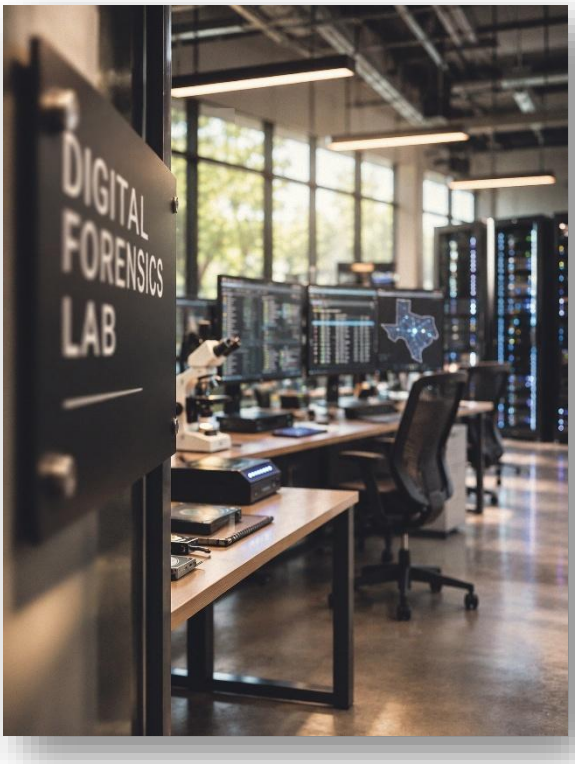
Direct monitoring coverage depends on the systems and telemetry connected to these services. Further integration and service expansion are being implemented in phases. The objective is to connect regional expertise with common technical capabilities so that findings from one incident can improve protection across participating entities. In addition, TXCC will commission a Continuity of Operations SOC (COOP SOC) in San Antonio co-located with TXCC headquarters location. This is structurally fundamental to statewide cyber operational readiness and cybersecurity resiliency.

Cybersecurity Incident Response Unit

In accordance with Texas Government Code § 2063.202, TXCC has established the CIRU as the primary capability for providing direct cyber incident response assistance during incidents affecting governmental entities and other covered organizations. The CIRU's mission is operational: rapidly assess an event, contain the threat, coordinate the necessary response resources, support eradication, and help restore affected services.

Digital Forensics Laboratory

In accordance with Texas Government Code § 2063.203, TXCC has established the DFL to provide the technical evidence and forensic-analysis capability behind incident response and cyber investigations. Its mission is to preserve and examine digital evidence, identify malicious artifacts and attacker techniques, and convert that evidence into findings useful for incident containment, recovery, intelligence, attribution, and potentially criminal investigation.



Cybersecurity Threat Intelligence Center



In accordance with Texas Government Code § 2063.201, TXCC has established the Cybersecurity Threat Intelligence Center (CTIC) as the agency's intelligence hub. Its purpose is to collect, analyze, contextualize, and disseminate cyber-threat intelligence so decisionmakers and operators have a better understanding of adversaries, their methods, and emerging risks.

The primary goals of the CTIC are to:

1. Provide context to circumstances surrounding Texas, national, or global cyber operations and threats.
2. Add clarity to decisions undertaken by the Governor, Legislature, and stakeholders across Texas.
3. Avoid surprise and drive prevention.

Information Sharing and Analysis Organization

In accordance with Texas Government Code § 2063.204, TXCC has established the Information Sharing and Analysis Organization (ISAO) as the statewide information-sharing and partner-engagement organization. Its core mission is to operate as a trusted, efficient, and effective clearinghouse through which governmental entities, critical-infrastructure organizations, institutions of higher education, and other partners can exchange threat information, analysis, best practices, and mitigation and remediation strategies.

Information sharing is crucial to reducing the quantity and impact of cyberattacks on entities within Texas. The TX-ISAO platform is available at no cost to all Texas entities, whether public, private, or non-profit. As of September 2026, more than 3,100 members of the TX-ISAO have access to entity and industry-specific cybersecurity intelligence, including information about current cybersecurity threats, attack vectors, indicators of compromise, educational opportunities, and other relevant security information.

From September 2022 to September 2026, the TX-ISAO distributed 2,482 cybersecurity notifications.[1] In addition to disseminating intelligence, the TX-ISAO collects cybersecurity threat information from members, analyzes trends, and issues notifications to improve the state's security preparedness and response capabilities. It also hosts monthly meetings to provide cybersecurity education and threat intelligence briefings.

[1] This measure reflects activity over the full period since September 2022 and is not limited to the report's principal reporting period.

Regional Security Operations Centers

Due to the complex cybersecurity landscape in Texas, a centralized security operations center might struggle to effectively address regional nuances. In 2021, the Texas Legislature authorized DIR to establish a pilot Regional Security Operations Center (RSOC). In April 2022, DIR unveiled the first RSOC in partnership with Angelo State University. In August 2023, following the program's success, additional RSOCs were established at the University of Texas at Austin and the University of Texas Rio Grande Valley.

In 2025, responsibility for the RSOC program transferred from DIR to TXCC under Texas Government Code Chapter 2063, Subchapter G. Together, the RSOCs provide regionally focused threat detection and response services while sharing observations and threat intelligence with TXCC's SOC to strengthen statewide cybersecurity.

The program also helps address Texas's cybersecurity workforce shortage by providing college students with hands-on experience under the supervision of cybersecurity professionals. Their efforts deliver threat monitoring, research, and mitigation services to eligible organizations. The three RSOCs currently provide opportunities for up to 150 students each semester to get hands-on experience protecting the state.

Together, Texas's Regional Security Operations Centers provide cybersecurity services to eligible local governments and schools, combining regional expertise, security monitoring, endpoint protection, vulnerability identification, and incident response with supervised student training. The current RSOC model is funded through base appropriations. The scaling necessary to strengthen service capacity, capability, and statewide reach will likely require a combination of general appropriations and cost recovery. As of September 25, 2026, reported results across the network include preventive services reaching at least 1,975 public entities across 248 counties, endpoint protection covering tens of thousands of devices, and interception of invoice-fraud attempts totaling nearly $8 million since April.

Volunteer Incident Response Team

The Texas Volunteer Incident Response Team (VIRT), authorized by Texas Government Code Chapter 2063, Subchapter F, is established to provide rapid incident response assistance to participating entities affected by a cybersecurity incident.

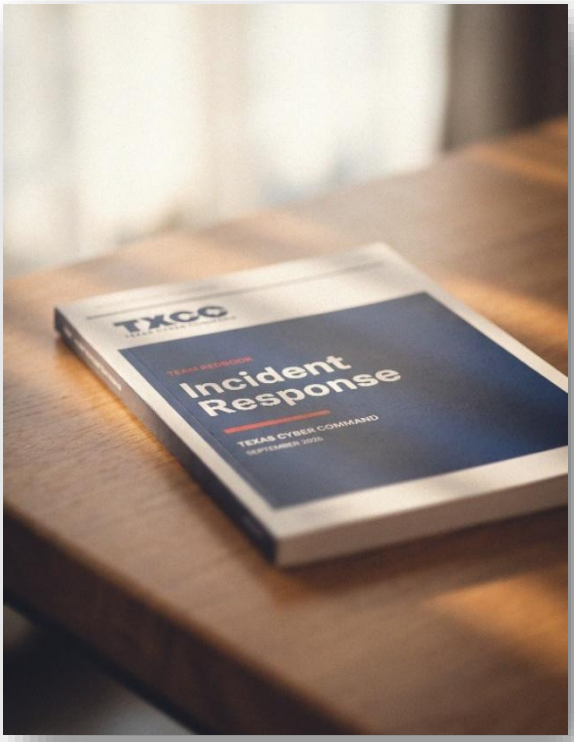
The VIRT comprises experienced and vetted volunteers who can quickly respond to significant cybersecurity incidents and provide support to eligible participating entities. Under TXCC's direction, capable volunteers provide support to participating entities in coordination with other state-level response resources.

Participating volunteers must be United States citizens, pass a background check, and sign a confidentiality agreement before activation. On request of a participating entity, TXCC may deploy

VIRT in response to a cybersecurity incident affecting multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event.

VIRT deployment capacity depends on verified volunteer eligibility, completed screening and agreements, relevant expertise, and availability for the incident.

Incident response practitioners with expertise in addressing cybersecurity incidents and technology administration may apply for membership on the VIRT by completing and submitting to TXCC for review a volunteer application. The VIRT meets quarterly to conduct cybersecurity training, provide threat intelligence updates, and socialize statewide cybersecurity initiatives, and it also offers members no-cost training through a third-party upskilling online platform. In a drive toward prevention, TXCC envisions a future wherein the VIRT could be mobilized in advance of need to raise the resiliency posture across the state in coordination with RSOCs.



Texas Cybersecurity Incident Response Plan

In response to increased cybersecurity incident activity, Texas Government Code § 2063.402 directs TXCC to develop a plan to address cybersecurity risks and incidents in Texas.

The plan was first completed in 2017 and updated in 2022. It is currently being revised to accommodate the wider scope of TXCC, documenting a statewide collaborative approach to responding to cybersecurity incidents.

Statewide Incident Response Preparedness

TXCC maintains a comprehensive Incident Response Team Redbook with included incident response plan templates for agency use. In addition to this document, TXCC also provides cybersecurity tabletop exercises to help government entities prepare for incident response activities.

The Incident Response Team Redbook provides a foundation for government entities to build their own internal incident response plan and capabilities, containing templates, guides, relevant legal references, and additional resources based on industry best practices that can be adopted and tailored to suit the unique needs of individual entities.

Members of the Texas Information Sharing and Analysis Organization (TX-ISAO), which is open to any entity in Texas, including state agencies, local governments, public and private institutions of higher education, and the private sector, have access to multiple customized tabletop exercise packages. These packages include a facilitator's guide, a participant situational manual, and a slideshow presentation to help guide exercise discussion. TXCC can also develop and facilitate custom tabletop exercises for entities based on their incident response plans.

Tabletop exercises offer entities the opportunity to discuss, practice, and rehearse the specific steps they would take to respond to a security incident while also documenting prospective improvements to their incident response plan.

Statewide Cybersecurity Incident Reporting

State agencies and institutions of higher education are statutorily required to report cybersecurity incidents. During the 88th Legislative Session, the Texas Legislature expanded the cybersecurity incident reporting requirement to include local government entities as defined in the statute. State agencies and local jurisdictions now report cybersecurity incidents to TXCC through a secure online web portal in alignment with statutory[2] and TXCC rule requirements.[3] These reports support TXCC's analysis of reported cybersecurity incidents and contribute to statewide awareness of cyber threats.

Cybersecurity incident reports received by TXCC include business email compromise, data exposure, and unauthorized system access affecting state and local entities. With this information, TXCC can track the cybersecurity incident trends across the state. This awareness allows us to share actionable information with TX-ISAO members via tailored security advisories that identify common attack methods, malicious indicators of compromise, and incident trends, shape preparedness activities, and determine cybersecurity education criteria.

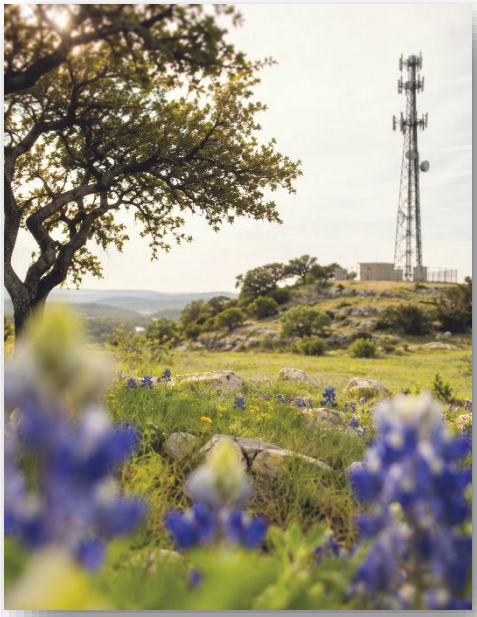
Cybersecurity Standards

TXCC sets the information security standards for state agencies and institutions of higher education, which are codified at 1 Texas Administrative Code Chapter 477. 1 TAC Chapter 477 establishes the minimum-security controls required for state information systems, which aligns with the National Institute of Standards and Technology Special Publication 800-53 (revision 5).

The Texas Cybersecurity Framework (TCF) helps organizations assess and improve the maturity of their cybersecurity practices. It organizes security control objectives under Identify, Protect, Detect, Respond, and Recover. The framework supports risk management and process improvement; it does not itself add regulatory requirements. Framework-based maturity

[2] Texas Government Code § 2063.302

[3] 1 Texas Administration Code § 477.21



assessment should therefore be distinguished from compliance with applicable information-security rules and control requirements. TXCC is presently assessing opportunities to update the TCF.

Critical Infrastructure Initiatives

TXCC has several critical infrastructure initiatives underway to bolster the state's cybersecurity posture in this vital domain.

Originally developed in July 2023 through a partnership between DIR and the Texas A&M Engineering Extension Service, the Introduction to Cyber Incident Investigation for Law Enforcement is administered by TXCC at no cost to law enforcement and non-commissioned staff who are eligible upon completion for four hours of Texas Commission on Law Enforcement credit.

Developed in 2025 through a partnership between DIR and the Texas A&M Engineering Extension Service, the Introduction to Cybersecurity for Water and Wastewater Systems course is administered by TXCC at no cost to industry professionals who are eligible upon completion for up to 4 hours of Texas Commission on Environmental Quality credit.

Developed in early 2026 through a partnership between DIR and Texas Tech University's Global Laboratory for Energy Asset Management and Manufacturing, the Cybersecurity Essentials for the Electrical Grid course is administered by TXCC at no cost for novice and intermediate personnel working in the power and energy field. It is designed to help participants prepare for the North American Electric Reliability Corporation Critical Infrastructure Protection certification.



TXCC is expanding the state's critical infrastructure cybersecurity capabilities through the development of the Critical Infrastructure Cybersecurity Center of Excellence (CI CCOE). Launched in April 2026, the CI CCOE represents a new statewide capability focused on strengthening cybersecurity across Texas's critical infrastructure sectors. The center seeks to better



understand the challenges facing critical infrastructure operators, improve statewide awareness of cybersecurity risks and needs, and develop the tools, resources, and support necessary to strengthen the security and resilience of critical infrastructure across Texas.

Finally, launching November 2026, Project Watershed 250 is a TXCC-led pilot in partnership with the White House Office of the National Cyber Director to strengthen cybersecurity for Texas water and wastewater systems. This pilot combines federal convening power, private industry capabilities, and state and local expertise. Watershed 250 advances TXCC's statutory mission by seeking to reduce cyber risk to essential water infrastructure, improving statewide visibility into common risks, and testing a repeatable public-private model that can strengthen other critical-infrastructure sectors. The goal of Watershed 250 is to build and test a model for shortening the time to assess and identify governance and technical vulnerabilities, reduce cyber risks, and determine costs to prevent, defend, and secure water utilities of different sizes. From these lessons, TXCC plans to scale the service model across Texas's water sector and other critical infrastructure sectors.

In addition to these critical infrastructure courses, TXCC shares sector-specific recommendations and resources through the TX-ISAO and relevant stakeholder associations.

State and Local Cybersecurity Grant Program

The federal Infrastructure Investment and Jobs Act was signed into law on November 15, 2021. An essential component of the Act is the State and Local Cybersecurity Grant Program, which appropriated $1 billion over four years (2022-2025) to selected grant recipients to address cybersecurity risk and threats to information systems owned or operated by or on behalf of state, local, and tribal governments. The program allocated Texas approximately $43 million to award over four years.

TXCC serves as the subject matter expert pertaining to all programmatic requirements and federal regulations associated with the State and Local Cybersecurity Grant Program. Facilitation of the program includes establishing a Cybersecurity Planning Committee, leading the

development of a Cybersecurity Plan, and assisting with identifying projects to implement for utilizing the provided funding.

Cybersecurity Education and Outreach

TXCC offers many free professional development webinars targeted to state and local government entities. In addition, TXCC partners with national technology and security consulting firms to conduct monthly webinars on security topics. In even months, TXCC hosts education security webinars presented by third-party vendors sharing timely topics, trends, and information for strategic planning.

Once a year, TXCC holds an Information Security Forum, which is an educational conference for public sector security and technology professionals from across Texas. Additionally, TXCC hosts an annual Information Security Officer Summit for officially designated Information Security Officers from state agencies, institutions of higher education, and public junior colleges. This annual education opportunity gives Information Security Officers a unique opportunity to meet each other face-to-face, collaborate on security initiatives, and discuss current security challenges facing the state.

Infosec Academy offers state information security teams a variety of professional cybersecurity certifications and trainings to enhance their cybersecurity capabilities and the overall cybersecurity posture of the state. The Legislature appropriates funding for TXCC to cover the costs for other state agencies, institutions of higher education, and public junior colleges. As of August 2026, 812 state employees attended a course through the InfoSec Academy, an increase of 461 participants since 2024. Additionally, participants completed 1,075 training courses, and 304 certification exam vouchers were issued to support participants in earning industry-recognized cybersecurity credentials.



Each October, in honor of Cybersecurity Awareness Month, TXCC hosts free in-person events and virtual presentations to raise awareness surrounding cybersecurity issues. Additionally, TXCC leverages social media to promote Cybersecurity Awareness Month, including posts about TXCC's security programs and resources and cybersecurity tips.

Cybersecurity Awareness Training

TXCC oversees the state's cybersecurity awareness training program required for most state and local employees. Texas Government Code § 2063.102 requires TXCC, in consultation with the Texas Cybersecurity Council, to certify at least five cybersecurity training programs for state and local government employees. Most state and local government employees must complete an annual training program certified by TXCC.[4]

TXCC certified 86 cybersecurity training programs for FY 2027. Additionally, TXCC received 4,609 compliance reports in FY 2026 from state and local government entities (63% of the 7,318 Texas state and local government entities). This represents a significant increase from the 34% compliance rate reported in 2024.

Texas Risk and Authorization Management Program

Texas Government Code § 2063.408 requires TXCC to establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. In support of this legislative initiative, TXCC established the Texas Risk and Authorization Management Program (TX-RAMP). Statute requires vendors contracting with state agencies to provide cloud computing services to be TX-RAMP certified and maintain compliance and certification with the program throughout the term of their contract with the state.[5] TX-RAMP provides a standardized approach to the security assessment of cloud computing services to reduce the risk of the state using third-party cloud services.

In 2023, TX-RAMP established a Fast Track certification option that reduces assessment time for certification by accepting certain third-party security artifacts recognized by the cybersecurity industry to be reasonable predictors of the security profile of a vendor. To date, TXCC has issued certifications for over 2,600 cloud services.

[4] Texas Government Code § 2063.103

[5] Texas Government Code § 2063.408 (d); *see also* Tex. Admin. Code § 477.27 and Tex. Admin. Code § 477.77.

Resources Assessment Summary

TXCC provides cybersecurity monitoring, incident response, forensic support, threat intelligence, assessments, training, and regional assistance through its own capabilities and delivery partners. These resources support prevention and recovery, while shared-platform integration and service expansion remain in progress. As of August 2026, endpoint detection and response services delivered through DIR's Managed Security Services program covered 496,214 devices at 473 eligible government entities. These figures describe that service and should not be interpreted as complete coverage of all systems at participating entities.

Available assistance depends on funded personnel, deployed technology, service agreements, and the demands of concurrent operations. Participating entities still need their own continuity arrangements, restoration capability, and funding for costs not covered by the assistance or services they receive. The grant program supports eligible projects over defined funding periods; its historical allocation is not a measure of incident-response funds currently available.

Texas Government Code § 2063.006 permits TXCC to request that the Governor or Legislative Budget Board propose emergency funding when an incident creates that need. This authority is a funding-request mechanism, not a dedicated incident-response appropriation or a guarantee of funding for a particular incident. Sustaining existing services and expanding capacity therefore require distinct funding decisions.

TXCC's filed FY 2028–2029 Legislative Appropriations Request comprises $243,397,595 in base funding and $234,984,376 in seven exceptional items, totaling $478,381,971. These are requested appropriations, not resources presently available for incident response.

The request includes $54,418,044 in General Revenue to replace historical cost-recovery funding supporting transferred cybersecurity services. That item sustains existing services rather than establishing a new program.

The related statutory clarification concerns the relationship among service funding, billing, and collections. The codified text of Texas Government Code § 2059.151 assigns DIR a billing system for network-security services provided by TXCC, and Texas Government Code § 2059.152(d) requires an agreement to transfer funds to TXCC. Texas Government Code § 2063.005 separately permits TXCC to recover service costs from covered entities when reasonable and practical. These provisions must be read with HB 150's transition provisions and the implementing agreements. TXCC recommends aligning these provisions to make billing and collection responsibilities explicit, explain how appropriated funding affects amounts charged for services, and clarify transfers of collected funds. The requested appropriation would replace a historical funding source; the statutory clarification would identify the continuing responsibilities for service funding and cost recovery.

Other Government Resources

Managed Security Services

DIR's Managed Security Services (MSS) help Texas government agencies, local government, municipal, and higher education customers strengthen their cybersecurity protections by making scaled managed security capabilities provided by a DIR contracted vendor available to these entities. MSS offers two core service categories, Security Operations Services and Risk and Compliance Services, designed to help customers protect their systems, respond to potential incidents, and improve their overall cybersecurity posture. Each category offers multiple individual services to help improve the security at the customer organization.

In the 88th Legislative Session, the Texas Education Agency received funding to enhance cybersecurity for K-12 schools and is partnering with DIR on this initiative to provide endpoint detection and response for interested K-12 schools.[6] Other Texas public entities, such as municipalities and counties, can purchase endpoint detection and response services through DIR's MSS program. As of August 2026, 473 eligible government entities obtained endpoint detection and response services from TXCC (delivered through DIR's MSS program), covering 496,214 endpoint devices.

Texas Identity and Access Management

DIR's Texas Identity and Access Management (TIAM) is the state's official Multi-Factor Authentication (MFA), single sign-on (SSO), and Identity and Access Management (IAM) assessment program. These services provide organizations with IAM Assessments — a tool to assess current state IAM solutions and provide recommendations for target state — and Texas Digital Identity Solution (TDIS) — a platform to deliver MFA and SSO to DIR customers.

As part of TIAM, TDIS supports MFA with hard tokens. This feature enhances security with a robust and easy-to-use MFA method. Each hard token is intended for use by a single user. TIAM offers hard tokens for organizations who are required to comply with Federal Information Processing Standards.

Existing Cybersecurity Statutes Review

Existing cybersecurity and information resources technologies statutes are predominantly located in the following Texas Government Code chapters:

- Texas Government Code Chapter 2054, the Information Resources Management Act;
- Texas Government Code Chapter 2059, the Texas Computer Network Security System; and
- Texas Government Code Chapter 2063, Texas Cyber Command.

[6] This partnership was transferred from DIR to TXCC upon establishment of TXCC.

These statutes identify points of collaboration between TXCC as the cybersecurity agency and DIR as the IT agency. Additionally, they establish and govern TXCC's cybersecurity and network security responsibilities and provide the statutory basis for the recommendations presented below, which include conforming corrections, clarification of existing responsibilities, proposed new authority, and funding requests.

Legislative Recommendations

TXCC submits the following recommendations for the Legislature's consideration.

Texas Cybersecurity Council Recommendations

Pursuant to Texas Government Code § 2063.406(f), the following recommendations are proposed by members of the Texas Cybersecurity Council and submitted to the Legislature for review and consideration.

Make the RSOC Program Inclusive to Texas Public Junior Colleges

Allow public junior colleges with established cybersecurity programs to host Regional Security Operations Centers (RSOCs), subject to TXCC requirements for secure facilities, qualified supervision, and operational capability to broaden regional service access and cyber workforce development.

Clarify Local Authority Over Internal AI Use

Clarify that local governments can set rules for how employees, officials, and contractors use, purchase, and secure AI tools and manage related records. Keep statewide limits on local AI regulation and existing privacy, confidentiality, and public-information requirements in place.

Simplify Cybersecurity and AI Training Compliance

Align definitions, reporting periods, and statutory references; assign cybersecurity training certification to TXCC and AI certification to DIR. Extend annual cybersecurity training to all state employees, agents, and contractors, with defined exemptions, and establish a uniform AI contractor training requirement.

Recognize equivalent certified training and allow one annual certification through a unified portal to satisfy equivalent contract and grant reporting for the same personnel, training, and period.

Require annual cybersecurity and AI training for school district cybersecurity coordinators and at least 25 percent of district staff who use computers according to a risk-based approach.

Align Eligibility for TXCC Cybersecurity Services

Align eligibility requirements so organizations authorized to receive cybersecurity services under an agreement with TXCC may also receive the Managed Security Services necessary to support those services.

Amend related network security and Regional Security Operations Center service eligibility statues to align to the "covered entity" eligibility reference for public and private organizations in Texas Government Code Chapter 2063.

Enable Secure Critical Infrastructure Information Sharing

Authorize public entities to share existing infrastructure data with TXCC and DPS to assess cybersecurity risks, identify critical dependencies, and evaluate the consequences of disruption. Enable timely information sharing before, during, and after cybersecurity incidents to support prevention, isolate affected systems, contain threats, and mitigate harm.

Require mission-limited use, secure access and handling, and establish controls on further disclosure. Preserve public access to information that is otherwise public under applicable law.

Authorize necessary safeguards to preserve applicable confidentiality protections and legal privileges and ensure compliance with federal restrictions governing sensitive information.

Expand Volunteer Incident Response Team (VIRT) Deployment Authority

Authorize the TXCC Chief or delegate to deploy the VIRT for incidents affecting a single participating entity under TXCC rules, retaining existing activation triggers.

Permit preparedness activities, maturity assessments, and technical assistance with the same protections and travel reimbursement policies as incident deployments.

Extend participating-entity eligibility to critical infrastructure operators.

Enforceable Minimum Cybersecurity Standards

Amend Texas Government Code § 2063.004 and § 2063.101 to clearly distinguish mandatory minimum cybersecurity requirements and establish a consistent, accountable process for addressing noncompliance.

Establish mandatory minimum cybersecurity outcomes for governmental entities, with implementation tailored to entity type, size, criticality, and risk. Provide reasonable implementation periods and assistance for entities with limited resources.

Authorize TXCC to assess compliance and require corrective action plans with risk-based deadlines. Provide notice of findings and an opportunity to correct or contest them. Include a method to document specific time-limited security exceptions with appropriate alternative safeguards and compensating controls subject to continuous reassessment and monitoring.

Protect sensitive findings and require reporting of material or repeated noncompliance to the entity's governing authority and appropriate oversight bodies.

Authorize temporary emergency directives for active exploitation or imminent, significant cybersecurity risks, with clear limits on scope and duration and requirements for notice, review, and termination.

Formalize Statewide Cybersecurity Tabletop Exercises

Amend Texas Government Code § 2063.402 to include an annual cybersecurity exercise requirement to expand private-sector participation in statewide cybersecurity tabletop exercises, including participation among critical infrastructure owners and operators.

Track that corrective actions and lessons are incorporated into operational plans and subsequent exercises.

Security Telemetry and Operational Data Access

Amend Texas Government Code Chapter 2059 and Chapter 2063 to ensure TXCC receives the timely security telemetry data needed to perform its statutory cybersecurity functions. Requiring state agencies to securely provide necessary security telemetry, asset and exposure information, and supporting event records.

Permit controlled sharing among authorized TXCC and RSOC personnel and affected participants while preserving confidentiality, need-to-know restrictions, and statutory audit access.

Limit collection and use to defined cybersecurity purposes and clarifying that data access alone does not authorize testing, containment, or system changes, while preserving existing lawful response authority.

Narrowly amend Texas Government Code § 2059.103(d) and § 2063.603(e) to permit sharing among authorized TXCC and RSOC personnel and affected participants for service delivery and incident coordination, while preserving confidentiality, need-to-know restrictions, and statutory audit access.

Texas Cyber Command Recommendations

The following TXCC recommendations carry forward the priorities identified in the Redundancies and Impediments section of the Agency Strategic Plan for Fiscal Years 2027–2031 and address additional operational needs and opportunities to strengthen statewide cybersecurity. Together, they provide the tools TXCC needs to deliver coordinated, cost-effective cybersecurity services, fulfill its statutory mission, and protect the essential systems Texans depend on every day.

Clarify Cybersecurity Training Requirements for State Agencies and Contractors

HB 150 transferred, redesignated, and amended the certified cybersecurity training provisions formerly in Texas Government Code § 2054.519 as Texas Government Code § 2063.102. It also transferred and amended employee and official training requirements as Texas Government Code § 2063.103. HB 3512 separately amended Texas Government Code § 2054.5191, including requirements tied to computer use for at least 25 percent of required duties. Legislation should reconcile these overlapping provisions and their cross-references.

TXCC recommends that training coverage extend to all state employees, agents, and contractors rather than being limited by the percentage of duties performed using a computer. Current requirements for certain state contractors are addressed separately in Texas Government Code § 2063.104 and should be reconciled with the proposed broader coverage.

Second, while DIR is responsible for state governmental entities' adoption of and training for AI, Texas Government Code Chapter 2063 should include a provision directing TXCC to develop a training module on the use of AI in cybersecurity.

Ensure Statutory Clarity for Criminal History Record Information

Criminal history access is addressed through provisions with different scopes. Texas Government Code § 411.0765(b)(26) addresses access to criminal history information subject to an order of nondisclosure for specified personnel providing Texas Government Code Chapter 2059 network-security services. Texas Government Code § 411.1404 expressly names DIR for personnel screening, while § 411.1405 provides a separate route for qualifying state-agency information-technology personnel.

TXCC recommends removing Chapter 2059 personnel limitation from § 411.0765(b)(26) and establishing an express TXCC personnel-screening provision corresponding to § 411.1404. The amendments should clearly cover employees, applicants, contractors, subcontractors, interns, and volunteers supporting TXCC's mission. This should be reconciled with HB 150's transition provisions and retain applicable safeguards for confidentiality, use, disclosure, retention, and individualized personnel decisions.

Authorize TXCC to Acquire and Deploy Cybersecurity Capabilities at the Pace of Emerging Threats

Texas's ability to prevent cybersecurity disruptions depends on deploying protection before vulnerabilities are exploited. As AI accelerates exploitation, purchasing timelines must support timely defensive action. Texas Government Code § 2063.007 provides limited purchasing exemptions for emergency incident response. TXCC recommends mission-specific authority for prevention, sustained operations, and shared service delivery when standard purchasing timelines cannot meet documented operational needs. This authority should enable timely action against rapidly evolving vulnerabilities and persistent cybersecurity risks without requiring an active incident or disaster declaration.

Amend applicable provisions of Texas Government Code Chapters 2054 and 2155, with conforming changes to Chapter 2157 as needed, to delegate cybersecurity purchasing authority directly to TXCC and establish targeted exemptions from centralized purchasing requirements. This authority should reflect TXCC's specialized responsibility for identifying the capabilities needed to protect Texas systems and critical infrastructure. § 2155.144 and § 2155.150 provide models for tailoring purchasing authority to agency responsibilities while retaining accountability.

This authority should cover both TXCC-funded purchases and agreements through which eligible participating entities may purchase common capabilities. It should permit deployment and authorized use by TXCC, RSOCs, delivery partners, and eligible entities, including within participant environments as part of TXCC's cybersecurity services.

These targeted changes would enable TXCC to act with speed and precision, strengthen operations across the state, and reduce duplicative spending. Authority should remain subject to appropriations, documented justification, procurement safeguards, and audit and legislative oversight, enabling Texas to prevent harm while preserving accountability for every public dollar.

Clarify Current Responsibilities Related to Prohibited Technology and Covered Applications

TXCC recommends a coordinated statutory framework for prohibited technology and covered applications that clearly identifies the responsible agencies and the requirements applicable to governmental entities. Amend Sections Texas Government Code § 620.003 and § 620.006 to expressly assign to TXCC, in coordination with the Department of Public Safety, the cybersecurity responsibilities for model-policy development, identification of risky applications, and publication of guidance and application lists. Reconcile those assignments with HB 150's transfer provisions and relevant executive direction, while preserving the Governor's designation authority and applicable exceptions and mitigating measures. The objective is consistent implementation without duplicate or conflicting agency instructions.

Clarify and Reconcile Statutory Cybersecurity Responsibilities

HB 150, Section 50, establishes the transfer of specified cybersecurity and network-security functions and addresses qualifying references in law to DIR. TXCC recommends conforming amendments that make the resulting responsibilities explicit in the codified provisions and distinguish transferred functions from duties retained by DIR.

The amendments should clarify cybersecurity roles in the advisory-committee provisions of Texas Government Code § 2054.033, § 2054.0333, and § 2054.0335; the digital-signature provisions of § 2054.060; and the security-reporting provisions of § 2054.068 and § 2054.069. They should also reconcile the overlapping information-security assessment and penetration-testing requirements in § 2054.5195 and § 2063.409. These changes should preserve DIR's unrelated information-resources responsibilities while removing inconsistent references and clarifying cybersecurity implementation.

Add TXCC to the List of Member Agencies Listed for the Homeland Security Council

Texas Government Code § 421.021 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. TXCC recommends adding TXCC to the list of member agencies listed for the Homeland Security Council.

Align Cybersecurity Service Funding, Billing, and Cost Recovery

Texas Government Code § 2059.151-152 address network-security charges, revolving fund deposits, and DIR-to-TXCC transfers. Separately, Texas Government Code § 2063.005 permits cost recovery for services to covered entities, and § 2063.004 (c) generally directs Chapter 2063 receipts to General Revenue. These provisions need clarification to align ongoing funding and billing responsibilities with HB 150 transfer provisions.

TXCC recommends amending Texas Government Code § 2059.151-152 along with conforming changes to § 2063.004(c) and § 2063.005 as needed in order to (1) assign responsibility for service billing, collections, deposits and interagency transfers consistent with HB150, Section 50 (d)-(e) and implementing agreements for TXCC's cybersecurity services; (2) align charges with appropriations by specifying which existing services General Revenue supports and preventing recovery of the same costs through appropriations and customer charges; and (3) preserve separate cost-recovery authority for covered-entity services under § 2063.005.

Establish CIRU Cyber Incident Scene Authority

Amend Texas Government Code § 2063.202 to provide TXCC's Cybersecurity Incident Response Unit (CIRU) clear authority to secure and control a cyber incident scene, stop ongoing harm, preserve evidence, and direct recovery. This recommendation equips CIRU to fulfill the mission the Legislature has already assigned by aligning its operational authority with its statutory responsibilities. Establish CIRU's incident response and investigative authority, limited to qualifying cybersecurity incidents and related offenses, and expressly authorize qualified personnel to control physical and digital access, require cooperation, preserve evidence, seek necessary legal process, and direct containment and recovery. Closing this operational gap would reduce delays that allow harm to spread, evidence to be lost, and essential services to remain disrupted, giving CIRU the tools to deliver the protection the Legislature intended and Texans expect.

Preventive and Recovery Efforts

TXCC provides the following action-oriented recommendations based on current cybersecurity threats observed across Texas state agencies, institutions of higher education, K-12 organizations, and local governments since the 2024 Cybersecurity Report. These recommendations are intended to strengthen Texas cyber readiness and resilience by reducing exploitable attack surfaces, improving detection and response capabilities, and supporting adoption of secure cloud and AI technologies while supporting alignment with the TCF and compliance with applicable state cybersecurity requirements.

Implement and Prioritize Identity Management

Identity compromise is a cybersecurity risk addressed by the preventive measures recommended below. Attackers increasingly bypass legacy Short Message Service (SMS) and push-based Multi-Factor Authentication (MFA) and instead use adversary-in-the-middle phishing kits and session-token theft. They also continue to target organizations with social-engineering tactics to trigger fraudulent password resets and MFA re-enrollment.

Dormant accounts, shared credentials, and inconsistent offboarding continue to create standing exposure long after an agency's relationship with an employee, contractor, or vendor ends.

Strategic Objective

Reduce the risk of identity-based compromise by enforcing phishing-resistant authentication, minimizing standing privilege, and continuously validating access.

Recommendations

- Require phishing-resistant MFA for users, remote access, and sensitive systems.
- Implement least-privilege access and risk-based conditional access policies.
- Automate onboarding/offboarding and perform periodic privileged access reviews.

Asset Visibility and Vulnerability Management

Effective cyber risk management depends on accurate, continuous visibility into an enterprise's IT and OT assets. Unmanaged and internet-exposed systems — including management interfaces on hypervisors, Virtual Private Network (VPN) appliances, and network edge devices — remain a primary entry point for both ransomware groups and nation-state actors, and the window between vulnerability disclosure and active exploitation continues to shrink. Shadow IT, unsanctioned cloud resources, and network and device configuration drift further erode the accuracy of asset inventories, leaving gaps that attackers exploit before they are ever assessed for risk.

Strategic Objective

Establish authoritative, continuously updated visibility into the enterprise attack surface and prioritize remediation by exploitability, exposure, and business impact.

Recommendations

- Maintain comprehensive inventories of hardware, software, cloud resources, identities, and external-facing assets.
- Continuously monitor for network and device configuration drift and unauthorized changes.
- Adopt risk-based vulnerability remediation using exploitability, exposure, and business criticality.

Cyber Resilience

Ransomware operators increasingly target their victims' backup infrastructure directly by deleting system snapshots, encrypting backup repositories, and targeting the hypervisor layer itself specifically to impede an organization's ability to recover without paying a ransom. Organizations that have not validated their restoration process under realistic conditions frequently discover recovery gaps only during an actual incident.

Strategic Objective

Ensure organizations can rapidly detect, contain, and recover from disruptive cyber incidents, including ransomware, without depending on attacker cooperation.

Recommendations

- Protect backup environments through isolation, immutable storage, and regular restoration testing.
- Maintain and exercise incident response and ransomware recovery plans.
- Define recovery objectives for critical business services and validate them regularly.

Modern Infrastructure Security

Hybrid IT environments require consistent security controls both on-premises and in cloud infrastructure. Cloud misconfigurations, flat internal networks, and internet-exposed management planes continue to be exploited by ransomware operators and nation-state groups alike, often as a direct path to hypervisor and virtualization infrastructure that underpins many other services.

Strategic Objective

Achieve consistent, verifiable cybersecurity controls across on-premises and cloud infrastructure while minimizing external exposure.

Recommendations

- Strengthen boundary defenses through network segmentation and reduced external exposure.
- Implement secure cloud architectures with centralized logging and runtime threat detection.
- Centralize security telemetry to improve detection and response.

Secure Software and Supply Chain

Software and vendor supply chains remain a significant and growing source of organizational cyber risk. A single vendor compromise can cascade across many downstream customers simultaneously, and internally developed applications that lack security testing or a documented software bill of materials create risk that is invisible until it is exploited.

Strategic Objective

Reduce risk introduced through internally developed software and third-party vendors by integrating security earlier in the lifecycle and holding vendors to defined security expectations.

Recommendations

- Integrate security throughout the software development lifecycle.
- Assess third-party risk and monitor vendor security posture.
- Require contractual security expectations and timely incident notification.

Governance and Continuous Improvement

Strong governance enables sustained cybersecurity improvement, but state oversight bodies have repeatedly identified a gap between documented compliance and actual operational cybersecurity maturity. Documented plans do not always reflect controls that have been implemented in production. Because control standards are updated on timelines measured in years, while cyber threat actors iterate in days, governance processes must support continuous, outcome-based cybersecurity improvements rather than moment-in-time compliance checks.

Strategic Objective

Close the gap between documented compliance and operational cybersecurity outcomes through clear ownership, standardized baselines, and recurring, evidence-based review.

Recommendations

- Assign ownership for key cybersecurity functions.
- Measure performance using outcome-based metrics rather than compliance checklists alone.
- Adopt standardized security baselines and conduct recurring governance reviews.

Security Operations and Threat Intelligence

A mature security operations function shifts an organization from reactive alert response toward proactive threat hunting informed by current, relevant threat intelligence. Organizations without adequate log coverage or tuned detection content often discover an intrusion only after a malicious cyber actor has dwelled within a network for some time, by which point containment and recovery costs are substantially higher.

Strategic Objective

Build a security operations capability that detects, investigates, and responds to threats within defined service levels, informed by continuously consumed and applied threat intelligence.

Recommendations

- Ensure security alerts are triaged and investigated within a defined service-level agreement.

- Produce and disseminate regular threat intelligence relevant to the organization's sector and geography.
- Conduct proactive threat hunts rather than relying solely on automated alerting.
- Continuously expand and validate log source coverage across critical systems.

Conclusion

Protecting Texas requires cybersecurity that anticipates threats, reduces vulnerabilities, and sustains the services Texans depend on every day. Growing digital dependence, persistent readiness gaps, and rapidly evolving threats make prevention a statewide imperative. TXCC is building the coordinated capabilities necessary to meet that responsibility.

The recommendations in this report establish clear priorities: sustain existing cybersecurity services, expand regional protection, strengthen the workforce, and align statutory authority with operational needs. Timely access to security information, targeted acquisition authority, and preparation for AI and quantum-related risks will strengthen Texas's ability to act before disruption occurs. Each organization must reinforce these statewide efforts through effective security controls, tested response plans, and demonstrated recovery capabilities.

Progress must be measured through reduced exposure, earlier detection, effective containment, and reliable recovery. Sustained legislative support, coordinated action across government and private industry, and accountability for results are essential to achieving those outcomes. TXCC's responsibility is to translate these commitments into measurable protection that keeps critical infrastructure secure, essential services running, and Texans safe.

Appendices

List of Acronyms

AI | Artificial Intelligence
BEC | Business Email Compromise
CI CCOE | Critical Infrastructure Cybersecurity Center of Excellence
CIRU | Cybersecurity Incident Response Unit
CISA | Cybersecurity and Infrastructure Security Agency
CTIC | Cybersecurity Threat Intelligence Center
DCS | Data Center Services
DDoS | Distributed Denial-of-Service
DFL | Digital Forensics Laboratory
DIR | Texas Department of Information Resources
FY | Fiscal Year
IAM | Identity and Access Management
ISAO | Information Sharing and Analysis Organization
MFA | Multi-Factor Authentication
MSS | Managed Security Services
PHI | Protected Health Information
PII | Personally Identifiable Information
RSOC | Regional Security Operations Center
SIEM | Security Information and Event Management
SMS | Short Message Service
SOC | Security Operations Center
SSO | Single Sign-On
TCF | Texas Cybersecurity Framework
TDIS | Texas Digital Identity Solution
TIAM | Texas Identity and Access Management
TPWD | Texas Parks and Wildlife Department
TXCC | Texas Cyber Command
TX-ISAO | Texas Information Sharing and Analysis Organization
TX-RAMP | Texas Risk and Authorization Management Program
VIRT | Volunteer Incident Response Team
VPN | Virtual Private Network

Glossary

AI | Artificial Intelligence, an artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

Cybersecurity Event | A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). Common and their impact is localized.

Cybersecurity Incident | A breach or suspected breach of system security, the introduction of ransomware into a computer, computer network, or computer system that jeopardizes information or an information system. Less common, but have higher impact to infrastructure, operations, and personnel.

Encryption | Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Financial Impacts | The immediate and long-term costs or financial losses resulting from a cybersecurity incident, including incident response, investigation, system restoration, disrupted operations, legal expenses, and regulatory penalties. Financial impacts may also include increased insurance costs and losses associated with reputational damage or impacts on public trust.

Incident Response Plan | The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber incidents and events against an organization's information system(s).

Independently Validated Operational Performance | An objective, third-party verification that proves that an organization stops threats and maintains resilience under world-world attack conditions.

Operational Impacts | The effects of a cybersecurity incident on an organization's ability to perform essential functions and deliver services, including system outages, loss of access to critical data, disrupted operational processes, and reduced staff productivity. Operational impacts may extend to third-party services, or dependent organizations, public safety concerns, and the effort required to restore normal operations.

Ransomware | A type of malware that is a form of extortion that works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Security Information and Event Management | Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

State Agency | A department, commission, board, office, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state, including a university system or institution of higher education

Technology | Information and communications technologies.

Third-Party Data Risk | The potential for data breaches, misuse, or other security incidents to occur due to vulnerabilities from an external third-party, such as a vendor, contractor, or service provider.

List of Figures

Figure 1 | Reported Agency Security Staffing and Contractor Positions, 2022, 2024, and 2026 Surveys 10

Figure 2 | Reported Biennial Trend in Agency Security Budgets, 2024 and 2026 Surveys 11

Figure 3 | Percent of State Agencies Who Report Having Adequate Resources Budgeted for Cybersecurity Incidents 12

Figure 4 | Frequency at Which State Agencies Review Cybersecurity Incident Response Plans ... 13

Figure 5 | Frequency at Which State Agencies Report Exercising Cyber Incident Response Plans 14