

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 engagement
- Cross-organizational collaboration
- Consensus building
- Change management
- Clear, concise communications
- Ethical judgement and decision-making



Part II: Workforce Analysis

CURRENT TXCC WORKFORCE

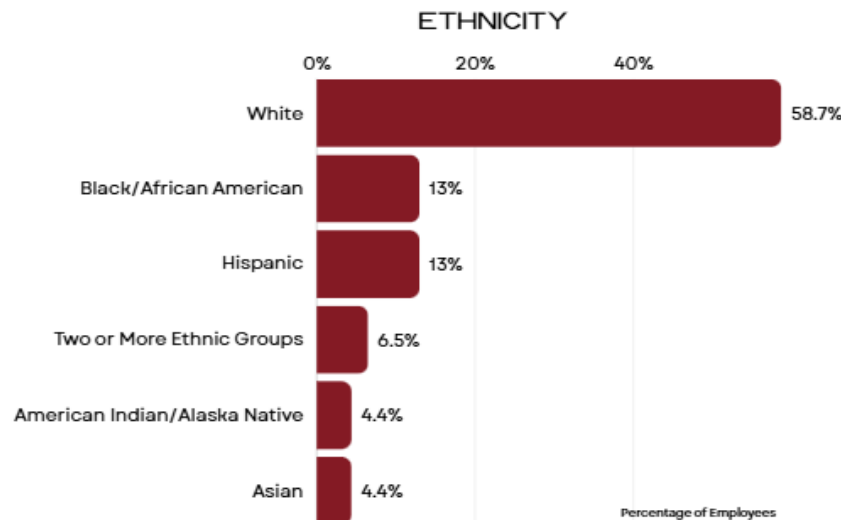
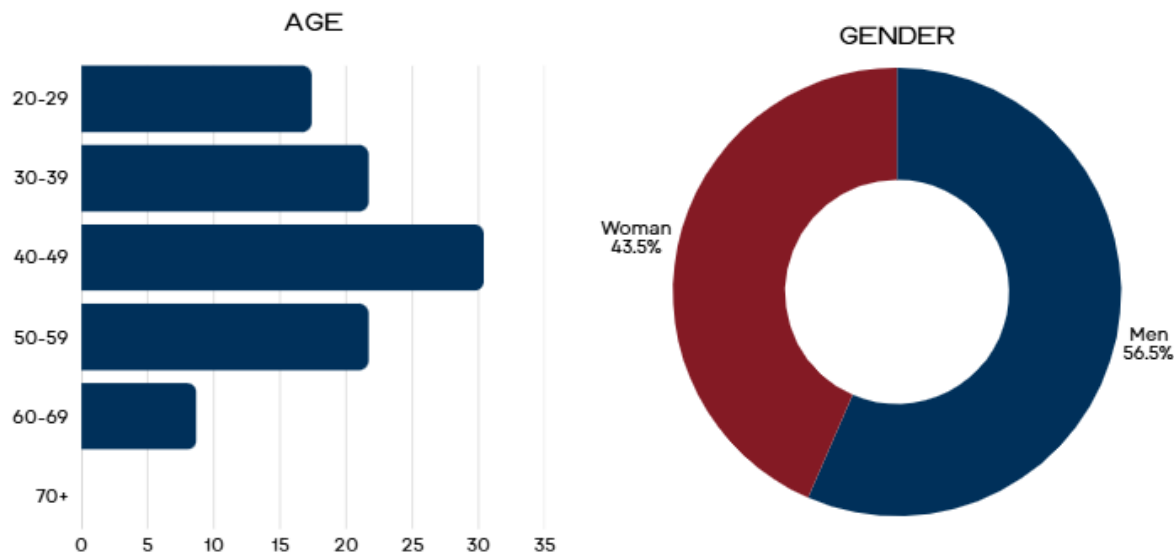
As a newly established agency, TXCC is in the early stages of building and assessing its workforce. As of May 2026, TXCC has a headcount of 48 full-time employees and is actively scaling toward an anticipated workforce of 122 employees, with a headquarters located in San Antonio and operational elements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

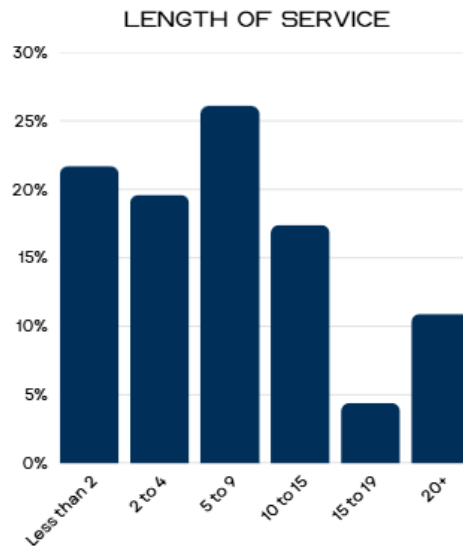
Age

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

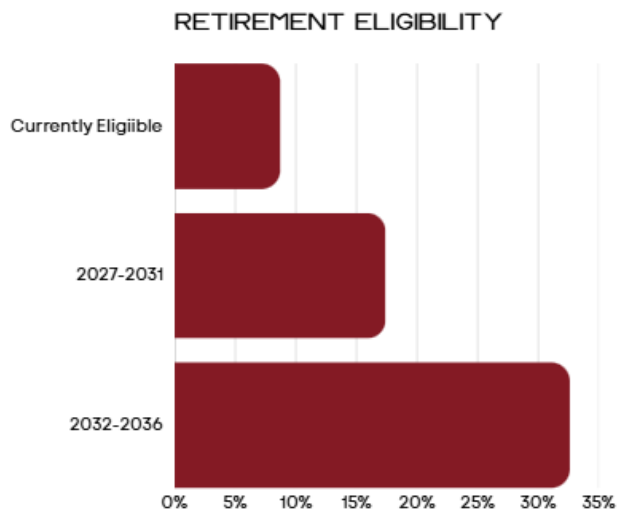
The TXCC workforce encompasses a strong concentration of mid-career employees, with 26% of the workforce having 5–9 years of service to the state. Employees with less than 5 years of service constitute 41% of the workforce, while 33% of the workforce have 10 or more years of experience and therefore 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 2025⁵, 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.