

Self-Evaluation Report

Submitted to the
Texas Sunset Advisory
Commission

August 31, 2023



Texas Department of Information Resources





Table of Contents

I. Agency Contact Information	1
II. Key Functions and Performance.....	1
III. History and Major Events.....	52
IV. Policymaking Structure	78
V. Funding.....	93
VI. Organization.....	107
VII. Guide to Agency Programs – Agency Administration.....	111
VII. Guide to Agency Programs – Communications Technology Services	154
VII. Guide to Agency Programs – Cybersecurity	173
VII. Guide to Agency Programs – Data Management.....	237
VII. Guide to Agency Programs – IT Procurement and Contracting	257
VII. Guide to Agency Programs – Shared Technology Services	289
VII. Guide to Agency Programs – Technology Guidance and Innovation	316
VII. Guide to Agency Programs – Texas.gov	351
VIII. Statutory Authority and Recent Legislation	367
IX. Major Issues.....	376
X. Other Contacts	395
XI. Additional Information	402
XII. Agency Comments.....	412
DIR Acronym List.....	416
List of Figures.....	421
List of Exhibits	423
List of Supplemental Attachments	423

Note: For the purposes of this report, the term “state agency” is used to indicate a state agency or a state-funded institution of higher education. The term “public entity” is used to indicate entities eligible for DIR services including local government, entities outside of the state, and others defined by Government Code.

Texas Department of Information Resources

Self-Evaluation Report

I. Agency Contact Information

Texas Department of Information Resources

Exhibit 1: Agency Contacts

Role	Name	Address	Telephone	Email Address
Agency Head	Amanda Crawford, Executive Director	300 West 15 th St., Austin, TX 78701	(512) 475-4775	amanda.crawford@dir.texas.gov
Agency Sunset Liaison	Brady Vaughn	300 West 15 th St., Austin, TX 78701	(512) 936-9640	brady.vaughn@dir.texas.gov

II. Key Functions and Performance

Provide the following information about the overall operations of your agency. More detailed information about individual programs will be requested in Section VII.

The Texas Department of Information Resources (DIR) is the cornerstone of public sector technology in the state of Texas. With approximately 250 current full-time employees who collaborate with industry partners to deliver a diverse set of services, DIR is a technology agency powered by people. DIR serves those who serve, and we are fiercely dedicated to our mission and vision.

Mission

The mission of DIR is to serve Texas government by:

-  Leading the state's technology strategy,
-  Protecting state technology infrastructure, and
-  Offering innovative and cost-effective solutions for all levels of government.

Vision

DIR's vision is to transform how Texas government serves Texans.

Core Values

To achieve DIR's mission and vision, DIR adopted a set of core values that are embedded in everything DIR does. These values are innovation, leadership, ethics, accountability, and

delivery, collectively known as **ILEAD**. These values guide employees in fulfilling their daily duties and aid executive leadership in decision-making.

Objectives

DIR's key objectives are to:

- Deliver an exceptional total experience to the public entities DIR serves and the entities with whom the agency interacts.
- Cultivate a compliance first culture throughout DIR and DIR's programs.
- Maximize value through the technology DIR provides so all levels of government can better serve Texans.
- Secure Texas through robust standards, innovative solutions, and strong partnerships.
- Promote operational excellence that sets the standard for state technology leadership.

The chart below summarizes DIR's strategic vision.

Figure 1 DIR's Strategic Vision

Business Objectives				
Exceptional Total Experience	Compliance First	Value Through Technology	Secure Texas	Operational Excellence
				
Strategic Goals				
• Improve ease of access to solutions and demonstrate business and fiscal value. • Partner with stakeholders to understand and address their needs. • Continue to evolve processes to improve customer and employee experience	• Provide compliance excellence through DIR's programs. • Evolve DIR's compliance-aware culture towards an enterprise risk management philosophy. • Continue development and adoption of comprehensive compliance standards and procedures to achieve excellence	• Enabling government innovation and cost efficiencies through technology solutions • Maximize value in IT services and solutions through rigorous and agile contracting. • Provide Texans with a positive and streamlined digital experience of government	• Deliver robust and forward-thinking security solutions to promote a secure Texas. • Promote security, data governance, and privacy awareness statewide. • Strengthen Texas' cybersecurity and incident response capabilities through partnerships across the state and nation.	• Continue to set the standard for government technology leadership and excellence. • Foster the DIR culture of adaptability, responsiveness, and mutual respect. • Lead the growth and development of a highly skilled, resilient, and vigilant state technology workforce.

Key Functions

DIR ensures that government entities, including state agencies, county and municipal

organizations, public colleges and universities, and K-12 education entities, can find and implement the most secure, innovative, and cost-effective technology available.

DIR helps public employees use technology to serve Texans more effectively by connecting them with innovative technology that is scalable and secure, while delivering the best value to taxpayers and the best service to the people of Texas. By statute,¹ DIR's Executive Director serves as the state's Chief Information Officer, charged with overseeing, supporting, and guiding state agencies' use of technology. DIR provides technology leadership and guidance to government entities and policy makers.

DIR protects the state's technology infrastructure and Texans' private data from cyberattacks and provides resources to help public entities improve their cybersecurity posture.

DIR has eight key functions that transform how Texas government serves Texans. Each of these functions are discussed in full detail in Section VII. To address the importance of these functions, DIR employs a cross-divisional approach where the functions are collaboratively achieved.

As described throughout this report, DIR provides an abundance of different services to many customers. While these services may be unique, they are not unrelated. All services that DIR provides fall under the greater umbrella of information technology. As reflected in Section III. History and Major Events, a key reason why the Legislature expanded DIR and its responsibilities was to accelerate the growth of information technology in the state of Texas. As technology evolves so does its reach, requiring a strategic and consistent approach to cybersecurity, disaster recovery, managed services, and the procurement of advanced technologies. The Legislature consolidated the strategic development of these approaches at DIR, ensuring a uniform approach to information technology in Texas that is more effective, resilient, cost-effective, and leads to the secure deployment of technology.

¹ [Gov't Code § 2054.0285](#).

Figure 2 DIR Key Functions



Agency Administration

DIR's Agency Administration function provides leadership and support for executing DIR's daily operations and mission. This function ensures compliance with laws and regulations; prevents and mitigates internal risks; recruits and develops DIR's workforce; manages agency finances and employees; secures and supports internal information systems and projects; and ensures the agency communicates the value of DIR programs to state leaders, other public entities, and stakeholders with holistic, unified, and consistent messaging.

Communications Technology Services

DIR's Communications Technology Services function empowers Texans to communicate with their government by providing a secure statewide network for data, voice, video, and internet to state agencies, education systems, and local government. Over 900 organizations use DIR's Communications Technology Services, which include offerings such as the Texas Agency Network (TEX-AN), the Capitol Complex Telephone System that serves 90 state agencies, and other high-quality communication technology services. DIR focuses on ensuring stable, secure, and reliable network operations while providing individualized customer service.

Cybersecurity

DIR's Cybersecurity function safeguards Texans' data and privacy by promoting cybersecurity best practices, guidance, and consultation; protects state information technology (IT) infrastructure; counteracts cyber threats; and responds with immediate assistance to government entities during a cybersecurity incident. Charged with more cybersecurity responsibilities than any other state agency, DIR is home to the state's Chief Information

Security Officer² and Cybersecurity Coordinator,³ who have statutory oversight for cybersecurity matters in Texas. DIR is responsible for protecting the State of Texas' network from countless cyber threats every day at the Network Security Operations Center, which serves as the headquarters for the state network's security services. As the internet provider for Texas' state agencies, DIR provides around-the-clock network security monitoring, alert notification, and analysis services, including proactively identifying potential cyber threats, issuing early warnings for attempted intrusions or cyberattacks, blocking known cyber threats to network security, and mitigating distributed denial-of-service (DDoS) attacks. DIR manages the development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and resolve network security incidents.

Part of the Cybersecurity function includes supporting other government entities when they are experiencing cyberattacks. For example, DIR's Cybersecurity Incident Response Team actively notifies entities of compromises found on the dark web and offers remote and onsite assistance to help state and local governments respond to and recover from cybersecurity incidents. Additionally, DIR operates the Regional Security Operations Centers, which partnerships between DIR and public universities to provide regional cybersecurity support and incident response for local government entities.

DIR helps entities prevent cybersecurity incidents by providing information security program guidance to state agencies, institutions of higher education, and other government entities. For the state, DIR sets information security policies and standards; publishes guidance on best practices; develops and improves incident response preparedness; monitors and analyzes incidents; provides cybersecurity training and skill development courses; coordinates state agency security assessments and penetration tests; offers cybersecurity awareness training; and promotes cybersecurity information sharing throughout the Texas public sector cybersecurity community. DIR also minimizes third-party cyber threats by certifying cloud service providers that have sufficient security controls in place for state agency and higher education use.

Data Management

DIR's Data Management function encourages a data sharing culture throughout state government and institutions of higher education. DIR coordinates the Texas Data Management Program to promote tools and best practices that improve data governance and integrity, while accelerating data management, sharing, and transparency.

Texas' Chief Data Officer is established in statute⁴ at DIR and is responsible for improving data governance and integrity statewide, seeking opportunities for data sharing across government, and working with agencies and institutions of higher education to collaboratively develop data

² [Act of September 1, 2023, 88th Leg., R.S., ch. 1079 \(S.B. 621\), § 1 \(to be codified as a new section at Gov't Code § 2054.510\).](#)

³ [Gov't Code § 2054.511.](#)

⁴ [Gov't Code § 2054.0286.](#)

policies, standards, and best practices, including enhancing interagency information coordination, reducing duplicate information collection, and increasing accountability for compliance with statutes and rules.

DIR administers and promotes the Texas Open Data Portal program.⁵ The Open Data Portal is the central repository of publicly accessible electronic data for Texas state agencies to publish high value data sets. These data sets increase state agency accountability and responsiveness, improve public knowledge, create economic opportunity, and respond to need and demand as identified through public consultation. Through the Open Data Portal, established in 2014, Texas government promotes transparency, enables resident self-service data participation, and makes efficient use of public resources. The portal offers over 800 publicly accessible datasets. As of June 30, 2023, it has registered 1,657,998 visits and supported 365,251 data downloads.

Information Technology Procurement and Contracting

DIR's IT Procurement and Contracting function leverages the purchasing power of the State of Texas to negotiate technology contracts and provide efficient and cost-effective IT products and services. DIR is the primary agency tasked with procurement of IT resources for Texas public entities.

DIR administers, procures, and manages the Cooperative Contracts program, through which billions of dollars of IT goods and services are procured each year. DIR negotiates master Cooperative Contracts to offer IT products and services at pre-negotiated discounts, terms, and conditions. Further, DIR reviews state agency statements of work valued at more than \$50,000 for compliance with statute and consistency with DIR's master contract language. Depending on various contract lifecycles, DIR has historically managed between 700 and 800⁶ Cooperative Contracts at a time, resulting in savings to the state through economies of scale and reduced administrative costs.

DIR leverages the state's buying power, offering statewide contracts for Shared Technology Services including Managed Security Services, the Texas Open Data Portal, Texas.gov, and Communications Technology services. In addition, DIR administers the lifecycle of the procurement for these services, which includes gathering customer input and requirements, posting the requests for offer (RFOs), evaluating vendors' responses, negotiating contract pricing, terms, and conditions, and awarding vendors the contracts. Once these contracts are awarded, DIR manages these contracts throughout their lifecycle.

DIR supports the state's Historically Underutilized Business (HUB) Program, which provides information and support to the HUB vendor community and monitors the use of HUB technology contracts. In Fiscal Year (FY) 2022, over 35 percent – or \$1.1 billion – of purchases

⁵ [Gov't Code § 2054.070](#).

⁶ The total number of Cooperative Contracts that DIR manages may fluctuate due to variances in the number of contracts DIR may award under different solicitations in a given year.

through DIR's Cooperative Contracts program were through HUB, a record in Texas.

Shared Technology Services

DIR's Shared Technology Services function enables Texas government to prevent unnecessary duplication of effort and services and reduces taxpayer costs by sharing technology services, collectively protecting technology assets, simplifying access to government services, and promoting the innovative and secure use of technology across the state.

DIR manages the Shared Technology Services, which are a set of managed IT services that Texas government organizations can use to accelerate delivery of their technology services in a reliable, modern, and secure manner. These services include Data Center Services, the Application Services Center, Managed Security Services, the Texas Open Data Portal, and Texas.gov Services.

- **Data Center Services (DCS)** delivers IT services through outsourced contracts, including public cloud services, private cloud services, mainframe services, security operations services, technology solution services, and print, mail, and digitization services. DCS began in 2005, when the Texas Legislature consolidated the state's technology infrastructure under DIR's two data centers, with 28 designated agencies required to use data center services.⁷ The program evolved into the Shared Technology Services and today more than 100 public entities receive Data Center Services.
- The **Application Services Center** includes the development, deployment, and maintenance of software applications, including the procurement, configuration, and integration of Software-as-a-Service (SaaS) and cloud computing services. The Application Services Center addresses the technology industry's evolution of software and infrastructure services into a combined SaaS technology and includes both infrastructure and application software. Additionally, it ensures that cloud-based applications connecting to or interfacing with the DCS environment are safe, secure, and properly managed for the good of the state's shared technology infrastructure. This includes leveraging the DCS program vendors to vet, procure, and integrate such products when they are adopted by DCS customers. Finally, the center encompasses Technology Solution Services, which provides strategy management, solution design, and project delivery in the DCS public and private cloud as well as application development services including development, maintenance, and staff augmentation services for applications hosted in the DCS public and private clouds.

⁷ [Gov't Code § 2054.382.](#)

- **Managed Security Services (MSS)** provides consistent, secure management of Texas' public sector data through security monitoring, device management, incident response, and risk and compliance management. MSS also assists eligible customers in consolidating security services, meeting legislative security requirements, and mitigating security risks. Today, 537 public sector entities receive MSS.
- The **Texas Open Data Portal's** contract management and customer outreach communications fall under the Shared Technology Services program, but the portal is part of the Data Management function described below.
- **Texas.gov Services** provides portal and payment services for Texas state agencies and eligible local government organizations, enabling them to conduct business online with their customers in a cost-effective manner via the state's official website. The program leverages enterprise-wide services and infrastructure components to provide solutions that meet or exceed state-mandated requirements regarding accessibility, security, privacy, and integration with the Texas Comptroller of Public Accounts. While the Shared Technology Services program manages the Texas.gov program and service providers, operating Texas.gov is one of DIR's main functions and more information is included in the Texas.gov function section.

Technology Guidance and Innovation

DIR's Technology Guidance and Innovation function presents a shared vision and goals for the state's IT resources so that agencies can align their own technology initiatives with broader statewide priorities. Through tracking and reporting on strategic priorities, DIR helps the Legislature prioritize technology investments. DIR coordinates several statewide programs to advance the use of industry best practices, innovative technologies, and the statewide project delivery framework. By providing awareness of emerging technologies, building collaborative communities, and offering tools, strategies, and standards, DIR helps state agencies position themselves as they embrace digital transformation and legacy modernization efforts, with the goal of ultimately delivering improved services to constituents. These programs work with state agencies and institutions of higher education to collaboratively develop policies that better serve the state.

Texas.gov

DIR's Texas.gov function is the state's official website and resource for Texans to access government information and conduct government business. Both constituents and Texas government entities benefit from DIR's implementation of Texas.gov.

For constituents, Texas.gov is a reliable source for Texas government information and guidance with online services, resources, and information about the state. Texas.gov provides hundreds of government services for residents and businesses including driver services, professional and occupational licensing, vital records, business resources, online payments, and more.

For Texas government entities, Texas.gov provides access to secure, payment card industry-compliant products that allow for online and over-the-counter payments with credit/debit

cards and Automated Clearing House (ACH) checks. Texas.gov provides services to over 300 state and local customers, processing constituent requests for items such as license renewals, registrations, vital records, and more.

Texas by Texas (TxT), the Texas.gov mobile-first digital assistant application, offers an additional way for constituents to complete government transactions in just a few clicks anytime, anywhere, and from any device. Since officially launching in January 2022, over five million constituents have created accounts on TxT and Texans can download the official app for use on their phone or other mobile device. Offered by Texas.gov Application Services, TxT enables government entities to integrate high-value, constituent-facing services on a centralized, account-based, and trusted platform. TxT is powered by a transformative technology platform featuring identity access management, predictive intelligence, and master data management technologies delivered to constituents as both a responsive web application and a mobile app.

TxT is a single, secure, and multi-factor authenticated user account and link service containing a personalized dashboard with upcoming to-dos, stored payment info, transaction history, and more. Texans can set up notification preferences to receive proactive alerts and reminders for when it's time to take action. TxT simplifies and coordinates government transactions like driver's license/ID renewals, vehicle registration renewals, and more in just a few taps.

**b) Do your key functions continue to serve a clear and ongoing objective?
Explain why each of these functions is still needed.**

Yes. Technology powers the business of Texas government and DIR is Texas' technology agency. DIR delivers the strategic thinking, purchasing power, and policy insights necessary to help public entities meet mission-critical needs and ensure that their use of information resources and technology is secure. Texans' demand for online interactions with government accelerated during the COVID-19 pandemic. During that same time, Texas state agencies rapidly implemented tools that facilitated expanded telework and remote learning, enhanced the use of data analytics, and empowered a more robust, secure, and modernized technology infrastructure for online government transactions. The increased use of technology by public entities and the desire of Texans for more online services shows no signs of slowing. Accordingly, while staying true to its enabling purpose of coordinating and directing the state's use of IT resources, DIR programs must meet the growing demands of Texas' public entities.

DIR ensures that government entities across the state of Texas can find, procure, and implement innovative and secure technology. DIR offers solutions that allow all levels of Texas government to leverage advanced and secure technology as a force multiplier to reduce costs while not reducing the level of services Texans receive.

Agency Administration

Yes. DIR's Agency Administration function provides leadership, support, and guidance to all other agency programmatic and functional areas that provide direct services to DIR customers and stakeholders.

Communications Technology Services

Yes. DIR's Communications Technology Services function ensures that Texas government entities using these services can communicate with their constituents, whether online or by phone. By purchasing telecommunications services through DIR, Texas government entities have access to highly competitive prices through the cost-effective purchasing power of the state of Texas. DIR's Communications Technology Services function streamlines procurement and ordering for Texas entities. When needed, DIR also assists state agencies with their DIR-provided internet, voice, and data network requirements.

Cybersecurity

Yes. DIR's Cybersecurity function is critical to maintaining the operation of Texas government and the protection of Texans' data. Cyber threat actors are becoming increasingly sophisticated and bold in their strategies, targeting government entities and the data they hold more than ever before. DIR's role in counteracting cyber threat actors and strengthening the state's cybersecurity posture grows every legislative session as the Legislature increasingly adds responsibilities, oversight, and resources that align with or supplement DIR's Cybersecurity function, affirming state leadership's trust in DIR's cyber capabilities. Since the Legislature charged DIR with creating a framework to measure state agencies' cybersecurity capabilities in 2013, state agencies' security maturity levels through both self-assessments and third-party assessments have continuously improved.

As cybersecurity threats emerge and evolve, DIR regularly updates required security controls for state agencies and institutions of higher education, public entity cybersecurity training, and required security standards for cloud computing services purchased by state agencies. DIR's cybersecurity end user awareness training prepares government employees—the front line of cybersecurity defense—to handle potentially malicious emails and thwart potential attacks. DIR's Infosec Academy ensures that state agency security professionals are aware of the standards and technologies required for protecting their organizations.

In the past two years, DIR offered support for 40 ransomware incidents, assisting Texas public entities during dire times of need. In that same time, DIR notified public entities of 281 vulnerabilities or system compromises that were discovered on the dark web or identified via other intelligence sources, providing technical support if necessary. Every day, DIR proactively blocks more than a billion cyberattacks on the state's network in addition to hunting the dark web for threats against government entities and operating an around-the-clock cybersecurity incident hotline for public entities needing assistance.

Data Management

Yes. DIR's Data Management function promotes a culture of data sharing in state agencies and institutions of higher education. The data that state government holds belongs to the people, and therefore, managing this data is a critical component of a trusted and reliable government. Managing data becomes even more significant as the government's data volume and complexity grows exponentially. In addition, the role of the state's Chief Data Officer will be increasingly essential in the future, as it promotes practices for improving state data

governance, preserving data integrity, and enhancing data management processes.

As the volume of data grows, Texas will need more robust governance mechanisms to uphold data integrity and enable efficient utilization. The state's Chief Data Officer will provide guidance and promote best practices, in alignment with the statutorily created Data Management Advisory Committee,⁸ to support these needs.

Furthermore, governmental efficacy turns on several issues, including the effective and secure interagency sharing of data and making public data readily available. Through its Shared Technology Services program, DIR provides state agencies, political subdivisions, and institutions of higher education with the tools for secure data sharing through the Texas Closed Data Portal and data transparency through the Texas Open Data Portal. The Texas Open Data Portal offers a centralized repository for open data that the public can access online 24 hours a day, seven days a week. As the amount of government-held data increases, the need for secure and open data sharing mechanisms intensifies. DIR's role in promoting data governance best practices remains central to Texas managing this data expansion effectively.

IT Procurement and Contracting

Yes. DIR's IT Procurement and Contracting function provides Texans with efficient and cost-effective IT products and services. Government entities are buying and utilizing more technology products and services than ever before. These entities are increasingly turning to DIR's contracts for IT products and services since they are pre-negotiated with strong state terms and conditions that comply with state law.

Entities bought over three billion dollars' worth of IT goods and services through DIR's Cooperative Contracts program in FY22—a 50 percent increase in just four years. In that time, DIR saved more than 3,900 Texas government entities—and, more importantly, Texas taxpayers—approximately 1.4 billion dollars in cost avoidance through negotiated price discounts.

DIR's IT Procurement and Contracting function saves government customers time and money, while providing assurances through contractual provisions that the data they hold will be secure and only accessible from within the contiguous United States, unless the customer expressly allows an exception.

Shared Technology Services

Yes. Shared Technology Services (STS) provides modern and secure IT infrastructure so state agencies can continue to deliver the services Texans expect. For Texas state agencies, cities, counties, universities, and school districts, a top priority is serving Texans. However, it can be difficult for many of these entities to get the IT resources and expertise required to deliver their services with quality technology that can do more for less.

⁸ [Gov't Code § 2054.0332](#).

STS strives to provide excellent value for taxpayer dollars in terms of the variety of robust services, security protocols, and industry-leading providers. Technology that was once feasible only for large organizations with significant budgets is now available to DIR customers of all sizes and backgrounds. DIR customers in STS save time and money, with competitively procured vendor contracts, in place and ready to go when they are.

STS started with a legislative mandate in 2005 with 28 participating agencies and initial, straightforward goals of infrastructure consolidation and modernization.⁹ As DIR and the program met its initial goals and customer demands increased, the program's focus pivoted to achieving the highest levels of security, reliability, and modernization available in the industry. Over the past 10 years, STS customer satisfaction rating among surveyed state agency business executives improved from 21 percent to 83 percent, proving the program is delivering its customers the right technology at the right time. As a result of its expanded offerings, as of August 2023, STS serves:

- 115 Data Center Services customers;
- 537 Managed Security Services customers;
- 79 Texas.gov customers;¹⁰ and
- 42 Open Data Portal customers.

STS provides robust security tools and protocols for keeping state information systems safe. With an added layer of security interwoven throughout the program, customers have the peace of mind that comes with knowing they have continuous protection with state-of-the-art security solutions.

As legacy systems create risks for the state, STS assists participating Data Center Services entities in updating and upgrading software and hardware to reduce the security and reliability concerns associated with legacy systems.

Texans' growing demand for online government services is driving digital transformation at the state level. STS facilitates an organization's digital transformation with modern technology at accessible prices.

STS provides entities with technical expertise and responsive support that frees up critical IT workforce resources for focusing on their organization's mission. At a time when state IT workforce turnover is tumultuous, outsourcing management of IT resources to STS ensures continuity and reliability for mission-critical tasks.

By taking advantage of STS, government entities can deliver the next generation of services to Texans quickly, securely, and cost-effectively. By joining STS, customers get the best the

⁹ [Gov't Code Chapter 2054, Subchapter L](#).

¹⁰ Count of Texas.gov services does not include the 254 counties that currently use Texas.gov under services that are leveraged by the Texas Department of Motor Vehicles.

industry—and Texas—has to offer.

Technology Guidance and Innovation

Yes. DIR's Technology Guidance and Innovation function provides statewide IT leadership by guiding, planning, and reporting on statewide IT priorities. One of DIR's original purposes was to set the strategic direction for information resources across Texas as the state began to increasingly depend upon technology. Today, Texas leaders look to DIR for guidance on establishing strategic priorities, modernizing legacy applications, implementing emerging technologies, and leading the state's digital transformation. DIR's Technology Planning and Innovation function provides state policymakers with centralized insights on IT implementation, best practices, and lessons learned across the state. For example, DIR collects information from state agencies about their risks and the potential impacts of failing to address their cybersecurity and legacy modernization projects for the Prioritized Cybersecurity and Legacy Report sent to the Legislative Budget Board that assists appropriators in budgetary decisions.

DIR's Technology Guidance and Innovation function helps agencies connect with emerging technologies to improve efficiency and service delivery. Planning today for tomorrow's government technologies ensures that state systems remain compatible, reduces unnecessary spending, and allows for adaptation.

Texas.gov

Yes. DIR's Texas.gov function is Texas' official one-stop access point for government information. Texans are increasingly interacting with government online and Texas.gov is their trusted resource to access government information and take care of government business in an easy, secure, and user-friendly way. Texas.gov provides services for more than 300 state and local customers.¹¹ In 2022, Texas.gov processed nearly 58 million transactions, totaling approximately \$2.3 billion for Texas government entities. As of August 2023, more than five million Texans have created a Texas by Texas (TxT) account and completed nearly nine million transactions with participating agencies including the Texas Department of Licensing and Regulation, Texas Department of Motor Vehicles, and Texas Department of Public Safety.

c) Does your agency's enabling law continue to correctly reflect your mission, objectives, and approach to performing your functions?

Yes. DIR's enabling law is the Information Resources Management Act, found in [Government Code Chapter 2054](#).¹²

The enabling statute recognizes that advancing technology provides the state with ongoing

¹¹ Count of Texas.gov services includes 254 counties that currently use Texas.gov under services that are leveraged by the Texas Department of Motor Vehicles.

¹² [Gov't Code Chapter 2054](#).

opportunities to deliver better, faster, and more cost-effective government services. This establishes DIR as the agency with the technology expertise to coordinate, plan, and provide guidance to avoid duplication of efforts and services and ensure the effective use of information and shared resources. DIR remains committed to providing technology resources for state agencies and public entities that leverage the state's collective buying power to maximize value and optimize service.

Still, technology has changed drastically since the Legislature added DIR's enabling statute in 1993, and while current statute continues to reflect DIR's mission, objectives, and approach to performing the agency's functions, updated and simplified enabling statutes that reflect current demands could help DIR better meet the needs of the public entities the agency serves.

DIR's enabling statute also recognizes that "state agencies' information and information resources possessed by agencies of state government are strategic assets belonging to the residents of this state that must be managed as valuable state resources."¹³ However, in 1993, the Legislature could not have contemplated the prolific, evolving, and well-funded cyber threats that now target those assets. Still, in the two decades since, the Legislature has, by appropriation and statute, given DIR significant responsibility to protect and defend Texas' information resources against cyber threat actors who seek to misappropriate those assets and disrupt government efficiency. Codifying in the enabling statute DIR's role as Texas' cybersecurity agency would solidify this authority.

d) Have you previously recommended changes to the Legislature to improve your agency's operations? If so, briefly explain the recommended changes, whether or not they were adopted, and if adopted, when.

Yes. DIR is statutorily required to provide recommendations to the Legislature in the Biennial Performance Report¹⁴ and the Biennial Cybersecurity Report.¹⁵

DIR's recommendations for statutory changes to improve the agency's operations are outlined below.

88th Legislative Session Statutory Recommendations

- **Local Government Cybersecurity Reporting.** State agencies and institutions of higher education are required to report certain types of security incidents to DIR, but local government entities do not have these same requirements. Requiring local entities to report cybersecurity incidents to DIR improves the state's ability to assist

¹³ [Gov't Code § 2054.001\(a\)\(1\)](#).

¹⁴ [Gov't Code § 2054.055](#).

¹⁵ [Gov't Code § 2054.0591](#).

recovery efforts and prevent future cyberattacks. The Legislature adopted this recommendation in [Senate Bill 271](#), which becomes effective September 1, 2023.¹⁶

- **Establish Statewide Privacy Officer.** Establishing a state Chief Privacy Officer role would provide state agencies a central point of contact regarding best practices and policy matters that involve data privacy and help government employees improve practices for the collection, use, and storage of personal, sensitive, or regulated data. The role would also educate Texans about the use of their personal information on mobile and digital networks, including steps they can take to help protect this information. The duties may include a biennial privacy review and resources for implementing best practices throughout Texas state government. More than 20 states have a statewide role to ensure that the privacy of their residents' personal information is protected. The Legislature considered this recommendation in [SB 782](#)¹⁷/[House Bill 984](#).¹⁸
- **Customer Alignment.** State law defines entities that are eligible customers for each of DIR's programs including DIR's statewide technology centers, telecommunication services, and Cooperative Contracts program. The definitions and eligible customer lists vary across state statutes and programs, resulting in increased research and analysis efforts for DIR's staff to ensure compliance without causing confusion for vendors and the eligible entities who use these programs. Streamlining the list of eligible customers across DIR's statewide technology centers, telecommunication services, and Cooperative Contracts program using uniform statutory definitions would provide clarity to DIR's customers and vendors that work with these programs. Additionally, removing the requirement for DIR to conclude that two or more customers want a product or service in the Cooperative Contracts program, or the Shared Technology Services program would allow DIR the flexibility to provide agency-specific products and services. The Legislature adopted this recommendation in [HB 4553](#), which becomes effective September 1, 2023.¹⁹
- **Statewide Technology Center Statute Update.** State law allows DIR to offer services through a statewide technology center only if it can do so to two or more government entities on a cost-sharing basis. The current state of both technology and the program render this requirement burdensome when customers need access to highly specialized applications and services. Additionally, [Government Code](#)

¹⁶ [Act of September 1, 2023, 88th Leg., R.S., ch. 267 \(S.B. 271\), § 1 \(to be codified as a new section at Gov't Code § 2054.603\).](#)

¹⁷ [Tex. S.B. 782, 88th Leg., R.S. \(2023\).](#)

¹⁸ [Tex. H.B. 984, 88th Leg., R.S. \(2023\).](#)

¹⁹ [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), §§ 1-16 \(to be codified as amendments to relevant sections of the Government Code\).](#)

[Section 2054.378](#) grants DIR authority to establish new statewide technology centers; however, it does not require that DIR define the scope of those offerings by rule to give state leadership, customer agencies, and vendors clarity and input into the establishment and offerings of any new statewide technology center.²⁰ The Legislature passed these recommendations in [SB 498](#), but it was vetoed by the Governor.²¹ [HB 4553](#) included the provision allowing DIR to provide services through the statewide technology centers to an eligible entity.²²

- **Chief Information Security Officer in Statute.** DIR's Chief Information Security Officer oversees the development and implementation of programs required by statute; the role, however, is not defined in state statute. Clarifying in statute that DIR employs a Chief Information Security Officer with oversight over state cybersecurity matters would align with current practices, other states, and industry standards. The Legislature adopted this recommendation in [SB 261](#), which becomes effective September 1, 2023.²³
- **Cooperative Contracts Program Update.** State law requires DIR to conclude that two or more customers need a product or service in order for DIR to make that service available under a Cooperative Contracts program contract. However, the current state of both technology and the program render the requirement burdensome when larger customers need access to highly specialized products and services. Additionally, DIR is charged by [Government Code Section 2157.068](#) to offer "technology services" under the Cooperative Contracts program, but the code does not define the term to provide clarity around the scope of services that can be offered.²⁴ This recommendation was filed as [SB 1125](#)²⁵/[HB 4552](#),²⁶ however, it was not adopted. [HB 4553](#) included the provision allowing DIR to provide products or services through the program in demand by an eligible entity.²⁷

²⁰ [Gov't Code § 2054.378](#).

²¹ [Tex. S.B. 498, 88th Leg., R.S. \(2023\)](#).

²² [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), §§ 2, 4-6 \(codified as amendments to relevant sections of the Government Code\)](#).

²³ [Act of September 1, 2023, 88th Leg., R.S., ch. 1079 \(S.B. 621\), § 1 \(codified as a new section at Government Code § 2054.510\)](#).

²⁴ [Gov't Code § 2157.068](#).

²⁵ [Tex. S.B. 1125, 88th Leg., R.S. \(2023\)](#).

²⁶ [Tex. H.B. 4552, 88th Leg., R.S. \(2023\)](#).

²⁷ [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 14 \(codified as an amendment to Gov't Code § 2157.068\)](#).

88th Legislative Appropriations Requests Adopted in the General Appropriations Act

- **Authority Only to Increase DIR Full Time Employee (FTE) Cap by 39 FTEs to 267 total FTEs.** Prior to the 88th Legislative Session, DIR conducted a zero-based budgeting initiative evaluating each division in the agency, their functions, and their spending to ensure that the agency is judicious in maximizing state funds. The review verified the significant increase of DIR's responsibilities over the years without sufficient additional FTEs to help maintain that workload. Since the 2013 legislative session, DIR's FTE count has remained relatively the same. Conversely, over the last 10 years, the Legislature has significantly expanded the responsibilities and programs managed by the agency. At the same time, the agency successfully increased the number of government customers using DIR's services, the number of products and offerings to meet the need of those customers, and the overall utilization of DIR services. Through this evaluation, DIR determined a critical need for additional staffing to ensure that the agency maintains its high standard of compliance and service delivery for all statutory functions, particularly in the Procurement and Contract Management Office and Chief Operations Office.
- **Expansion of the Regional Security Operations Center Program (RSOC).** In 2022, DIR established the first RSOC at Angelo State University. DIR is currently taking the next steps to establish two additional RSOCs at the University of Texas at Austin and University of Texas Rio Grande Valley. DIR chose these two universities for the second iteration of the RSOC program in part to take advantage of the economy of scale. The proposal allows the regional security operations center and toolsets at the University of Texas at Austin to also be used at the University of Texas Rio Grande Valley, thus reducing the number of onsite capital expenditures, saving state funds without decreasing the capabilities of each individual RSOC. The expansion of this program will help to provide crucial cybersecurity services in the regions of the state where those universities are located. The RSOC program assists local governments, such as cities, counties, and independent school districts, with services including information security policies and planning, education and program support, assistance with infrastructure improvements, monitoring of network traffic and endpoints, and enhanced response capabilities.
- **Authority to Develop an e-Procurement System for the Agency.** DIR is responsible for providing state agencies and other eligible public entities with IT guidance and solutions that assist in accelerating service delivery in a reliable, modern, and secure manner. However, the agency's current procurement system was not developed to support modern contracting needs; it lacks the scalability necessary to support customer demand—both from a capacity and capability perspective. Transitioning to a new e-procurement solution will allow the agency to adapt the procurement process to meet the evolving legislative and audit requirements in real time.

- **Vendor Sales Reporting System.** DIR receives a large portion of its funding for operations from the Cooperative Contracts program administrative fees, which are calculated from the sales that vendors report using the legacy Vendor Sales Reporting (VSR) Portal. Upgrading the VSR Portal ensures that DIR receives the data necessary to accurately collect vendors' administrative fees, a key source of funding for the agency.
- **Funding for Retaining Cybersecurity Logs for Advanced Persistent Threats (APTs) Investigation.** APTs—which are usually nation-state actors from all over the globe—are constantly targeting the state of Texas. APT groups operate very slowly and with careful intent over several months to work their way into a network. DIR's Cybersecurity Operations team depends on logs from security tools to investigate suspicious network activity, which are key to finding an APT group's initial attack vectors. Traffic logs on the state network are the only tool available to find previous activity associated with an APT. The funding received for increasing the period of log retention helps improve the state's ability to investigate APT activity and protect Texas' networks from nation-state actors.
- **Supplemental Funding for Texas.gov Security Upgrade.** Texas.gov is the official website of the state of Texas. In 2022, cyber threat actors exploited the driver's license system through online portals, highlighting the need to exponentially expand the security and ability to verify the customers utilizing online state services. As the threat landscape is ever-evolving, Texas needs to adapt to those new threat vectors and rapid technology advancements.

87th Session Statutory Recommendations

- **Regional Security Operations Centers (RSOCs).** Establishing RSOCs located in different geographic regions throughout Texas to assist with cybersecurity incidents would allow for a first line of defense close to local government entities. This first line of defense can assist with cybersecurity incidents in each region, as well as provide network security infrastructure that regional governments can utilize. Hosting the RSOCs in public institutions of higher education also allows student workers to receive real-world training for the needed cybersecurity professionals of the future. The Legislature adopted this recommendation in [SB 475](#).²⁸
- **Volunteer Incident Response Team (VIRT).** Establishing a team of vetted volunteers into a VIRT under DIR to assist with responding to cybersecurity incidents would create a framework for a shared talent pool to assist with responding to events statewide. The Legislature adopted this recommendation in [SB 475](#).²⁹

²⁸ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\), § 9 \(codified at Gov't Code Chapter 2059, Subchapter E\).](#)

²⁹ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\), § 6 \(codified at Gov't Code Chapter 2054, Subchapter N-2\).](#)

- **Cybersecurity Training Enhancement.** Aligning cybersecurity training and requirements for state and local entities will help ensure that all entities working on public resources will have standardized security training. The Legislature adopted this recommendation in HB [1118](#).³⁰
- **Authority to Connect.** State agencies should require entities that access, transmit, utilize, or store state data to periodically provide evidence to the state agencies that the entities meet the defined security requirements. State agencies should review this evidence and determine if the contracted entities are issued an authority to connect, granting that entity permission to access, transmit, utilize, or store the state data as per the contract they are executing. Entities that fail to provide sufficient evidence should be required to remediate any shortcomings or lose their authority to connect. The Legislature adopted this recommendation in [SB 475](#).³¹
- **Risk and Authorization Management Program (RAMP).** Establishing a RAMP at DIR would provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for those vendors providing service to Texas state agencies. The Legislature adopted this recommendation in [SB 475](#).³²
- **Data Management.** Requiring agencies to publish all public, high-value data sets to the Texas Open Data Portal and perform an assessment of their agency's data program to determine gaps in data management will strengthen data management and transparency in Texas. The Legislature adopted this recommendation in [SB 475](#).³³
- **Texas by Texas (TxT).** Requiring state agencies to use the TxT digital assistant mobile application provides Texans with a secure, centralized, mobile-friendly portal for interacting with state government. The Legislature adopted this recommendation in HB [3130](#).³⁴
- **Cooperative Contracts Program Update.** State law restricted DIR to only offering products and services in demand by two or more agencies. Allowing DIR to provide products and services in demand by two or more eligible customers provides local government customer input into the program's offerings. The Legislature adopted this recommendation in [SB 538](#).³⁵

³⁰ [Acts 2021, 87th Leg., R.S., ch. 51 \(H.B. 1118\), §§ 2, 3, 5 \(codified at Gov't Code §§ 2054.519, 2054.5191\).](#)

³¹ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\) § 4 \(codified at Gov't Code § 2054.138\).](#)

³² [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\), §§ 2, 11 \(codified at Gov't Code § 2054.0593\).](#)

³³ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\), § 4 \(codified at Gov't Code § 2054.137\).](#)

³⁴ [Acts 2021, 87th Leg., R.S., ch. 270 \(H.B. 3130\), § 1 \(codified as an amendment to Gov't Code § 2054.113\).](#)

³⁵ [Acts 2021, 87th Leg., R.S., ch. 83 \(S.B. 538\), § 1 \(codified as an amendment to Gov't Code § 2157.068\).](#)

- **Local Reporting.** State agencies and institutions of higher education are required to report certain types of security incidents to DIR, but no such requirement exists for local government entities. Requiring local entities to report cybersecurity incidents to DIR would improve the state's ability to assist recovery efforts and prevent future attacks. This recommendation was filed as HB [4395](#) but not adopted.³⁶

87th Session Legislative Appropriation Requests Adopted in the General Appropriations Act

- **Regional Security Operations Center (RSOC) Pilot.**³⁷ Provides funding for DIR to partner with a Texas public university to establish the pilot RSOC.
- **Endpoint detection and response (EDR) technology.**³⁸ The General Appropriations Act grants DIR funding to purchase and implement EDR technology at no cost for all state agency issued computers, laptops, servers, and other endpoints to better protect from ransomware and other cyber threats.
- **Rider 11 Change.**³⁹ The General Appropriations Act allows DIR to perform a method of finance swap to fund cybersecurity services with collected revenue and transfer general revenue back to the treasury when revenues are sufficient to do so.

e) Do any of your agency's functions overlap or duplicate those of another local, state, or federal agency? Explain if, and why, each of your key functions is most appropriately placed within your agency. How do you ensure against duplication with other related agencies?

No other federal, state, or local agencies provide the scope of services and functions that DIR offers to other public entities, nor do other agencies help public entities achieve the same cost-saving margins for technology products and services as DIR. Other agencies do perform cybersecurity and procurement functions, and this overlap is described in the program sections of those functions.

f) In general, how do other states carry out similar functions?

Most states have a designated technology division or department whose authority, scope, and organization varies. State governments organize their IT functions using different approaches including centralized, decentralized, and federated models. These models represent various levels of control, decision-making, and resource allocation throughout the organization or enterprise.

³⁶ [Tex. H.B. 4395, 87th Leg., R.S.\(2021\).](#)

³⁷ [General Appropriations Act, ch. 1053 \(S.B. 1\), Art. IX, § 18.37 \(Contingency for Senate Bill 475\).](#)

³⁸ [Supplemental Appropriations Act, ch. 7 \(H.B. 5\), § 11 \(Department of Information Resources: Cybersecurity\).](#)

³⁹ [General Appropriations Act, ch. 1053 \(S.B. 1\), Art. I, § 11 \(Fund Balance Limitations\).](#)

Texas' federated model works well for a large state with diverse needs and department functions. The federated model provides shared aspects of IT management and policy oversight of the statewide IT function with other functions managed by the individual government entities. This model provides benefits of standardized guidance and some centralized control, particularly through the consolidation of most IT infrastructure, with the flexibility and customization offered by a decentralized approach.

Several states use a centralized model wherein they organize their state government's technology department under a single, unified authority. IT strategy, planning, procurement, infrastructure, and service delivery are centrally managed and controlled in these states. This model can lead to economies of scale but is less flexible and responsive to the specific and unique needs of individual departments and agencies.

Leadership and Strategy

DIR's statewide leadership roles include the state Chief Information Officer, the state Cybersecurity Coordinator, the state Chief Information Security Officer, and the state Chief Data Officer, all of which are statutorily created positions⁴⁰ with statewide oversight. Many other states have similar statewide leadership positions. Most states have a state Chief Information Officer (CIO) or an equivalent senior executive that plays a role in overseeing technology operations and strategy. Some states refer to this role as the Chief Technology Officer, or Commissioner or Secretary of IT/Technology.

[All 50 states](#) have a Chief Information Security Officer and more than half of the states have a Chief Data Officer. While Texas currently does not have a Chief Privacy Officer, 21 states do. Many of these technology leaders report directly to the state's governor in a cabinet level role. In Texas, DIR is governed by a 10-member Board of Directors, seven of whom are appointed by the Governor. The DIR Board hires an Executive Director who is the state CIO and has authority for:

- The use of technology to support state goals;
- Functional support to state agencies;
- Technology purchases;
- Deployment of new technology;
- Delivery of technology services; and
- The provision of leadership on technology issues.

Procurement and IT Service Delivery

The "Texas Model," as other states call DIR's IT procurement and service delivery program, is generally considered to be the closest governmental approach to privatized IT in the country. From a service delivery perspective, DIR has adopted a "CIO-as-a-broker" model wherein DIR offers managed outsourced services for its IT delivery. By doing so, the burden of maintaining

⁴⁰ Gov't Code §§ [2054.0285](#) – [2054.0286](#); [Act of September 1, 2023, 88th Leg., R.S., ch. 1079 \(S.B. 621\), § 1 \(codified as a new section at Gov't Code § 2054.510\)](#).

and operating a continually evolving and innovative technology program that can scale to the needs of Texas is shifted operationally from DIR to DIR's contracted service providers. This model helps to mitigate the significant risks of recruiting and retaining a technical state IT workforce capable of running a program of Texas' magnitude. For example, other states with a centralized and in-house approach have several times the magnitude of IT position vacancies than DIR has total FTEs. Rather, DIR is staffed with professionals skilled in technology, procurement, contract management, vendor management, and customer service to ensure our service providers are meeting DIR's rigorous service level agreements. This service delivery model is explained in more detail in the Shared Technology Services and IT Procurement and Contracting functions.

Several other states have reached out to DIR to learn more about how to transform the technology structure in their states to more closely mirror what we have here in Texas. Additionally, other states are increasingly using DIR's Cooperative Contracts program to address their own IT needs.

According to the National Association of State Procurement Officials (NASPO), only Texas and South Carolina delegate IT procurement to individual state agencies, with South Carolina delegating all authority to individual agencies. Even so, no other state has a technology cooperative program that rivals Texas. Since 2019, more than 570 out-of-state governments (including 44 other state governments) have utilized DIR's contracts, and the sales from out-of-state customers grew more than 129 percent in four years, which, in turn, benefits Texas.

NASPO data shows that 28 states procure IT through their state's central procurement office; 13 states share oversight of IT procurement between an agency and the state's central procurement office; and seven states procure IT through their state's technology department. These numbers, however, disguise a great deal of nuance in individual state approaches.

Although the majority of states have relatively centralized IT procurement authority, an estimated 65 percent of states have at least some degree of decentralized authority over IT procurement. In many of these states, authority over IT procurements was either:

- Delegated to individual entities if the procurement fell below a certain threshold or met certain specified criteria; or
- Vested in the state's Chief Information Officer (or similar role), even if ultimate responsibility for the procurement was vested elsewhere.

According to at least one study,⁴¹ around 66 percent of states grant their CIO (or similar role) some level of authority over IT procurements, even if the procurement authority itself resides elsewhere. Only 31 percent of states grant their state's CIO no authority whatsoever over state

⁴¹ Megan R. Smyth and Meredith Ward, *State IT Procurement Negotiations: Working Together to Reform and Transform* (2017), *available at* <https://www.nascio.org/resource-center/resources/state-it-procurement-negotiations-working-together-to-reform-and-transform/>.

IT procurements while only approximately 12 percent of states vest such authority solely in the CIO. While Texas does share common factors with the approach of other states, Texas' federated procurement model is unique in the nation.

g) Discuss any changes that could impact your agency's key functions in the near future (e.g., changes in federal law or outstanding court cases).

DIR's key functions are most likely to be impacted by the rapid growth and development of information resources and technology and the expansion of cyber threats in response to such technological growth. Technology is not going away nor are the demands for technological innovation from those government serves, and as a result, any changes in the technology field will impact DIR.

The potential changes most likely to impact DIR's key functions can be broken down into four separate subcategories:

- Emerging Technologies and Innovation;
- Legal Developments at the Federal and State Level;
- Cybersecurity Necessities; and
- Supply Chain Impacts.

Emerging Technologies and Innovation

DIR's mission is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. To fulfill this mission, DIR provides vision and guidance for Texas government through technology policy, planning, and standards that help promote consistent and effective use of technology across the state. As technology rapidly advances in the state of Texas, state leadership and agencies, institutions of higher education, local governments, and Texans alike look to DIR to provide leadership and guidance addressing the evolving expectations and needs of the state agencies and Texans that DIR serves.

Among these, state agencies and Texans expect government to incorporate emerging technologies, which have the potential to improve how government provides services to its constituents. However, agencies, including DIR, must weigh the benefits of incorporating emerging technologies against the risks to security and data privacy to ensure that government is ethically, responsibly, and economically using taxpayer funds to address the needs of the state.

Emerging technologies require state agencies to take a balanced approach that provides state agencies the opportunity to take advantage of these innovative tools while managing the disruptive effects of and risks for state agencies and individuals using new technology.

Furthermore, DIR's own function in incorporating innovative technologies at the state level is impacted as technologies evolve at a rate far faster than the legislative cycle can address, often leading to a disconnect between DIR's explicit statutory authorization and the demands placed upon DIR by state agencies and Texans to incorporate new technologies.

Examples of technologies that could impact DIR's key functions include:

- Generative Artificial Intelligence (AI), a term that includes tools that use prompts to create text, images, voice, and videos, has tremendous application opportunities and capabilities for state government. AI must be evaluated thoroughly, however, to ensure that concerns are addressed properly, and that the technology is implemented in a responsible and ethical manner.
- Blockchain technology, which is a decentralized, distributed, and public digital ledger that is used to record transactions across many records so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network, has significant potential to enhance the security and transparency of and accountability for records. State agencies interested in using blockchain technology must make many decisions, including determining whether blockchain-based systems are fiscally viable due to the substantial investment required at the outset, an intrinsic understanding of the technical architecture of their applications and networks, and a willingness to embrace the steep learning curve associated with using distributed ledger technology. As the technology and cybersecurity agency for the state, DIR has been called upon to serve on the Work Group on Blockchain Matters to develop a master plan for the expansion of the blockchain industry in Texas and to recommend policies and state investments in connection with blockchain technology. DIR will continue to monitor best practices for and provide guidance on the implementation, use, and security features required for applications using blockchain technology in addition to establishing any administrative rules and addressing any statutory requirements imposed upon DIR. In addition, the Legislature and state agencies would be required to update statutory authorizations and administrative rules to permit for the use of peer-to-peer (P2P) technologies like blockchain by Texans to conduct financial transactions with the state, and which would require DIR to update payments permitted by the Shared Technology Services program.

Legal Developments at the Federal and State Level

Because technology moves so rapidly, federal and state agencies and legislation are constantly trying to catch up to it. Federal and state governments have sought to impose greater controls over the use of emerging technologies. Potential legislation or shifts in control standards could impact DIR's key functions in the following ways:

- Increased federal oversight of AI may impose new standards upon the use of AI that DIR would then have to follow. These standards may result in increased costs to DIR or the entities to which it provides services.
- Federal data security programs like the Federal Risk and Authorization Management Program (FedRAMP) and Criminal Justice Information Services may impose more restrictive federal controls. If these controls were more restrictive than those DIR already requires, DIR may be required to invest more in cybersecurity, potentially

restrict data sharing, or overhaul Texas' systems or network to comply. These necessary changes could ultimately result in an increase in the costs of services or products and may limit market choice for state agencies and institutions of higher education.

- Privacy issues are also becoming a matter of significant legislative discussion, which could result in changes to state and federal law to address these concerns. Changes in federal and state privacy laws could require DIR to limit or otherwise require expansive consent to permit constituent data collection, storage, usage, sharing, and deletion. Dependent upon the legislation, Texas state agencies may need to update data practices and modify existing systems and applications to be compliant with the applicable privacy laws, which could require expensive modifications to several of the state's largest applications.

Changes in funding rules, updates to industry standards and guidance, or terms and conditions associated with funding that DIR receives to support its programs could also impact our key functions. These include:

- Governmental Accounting Standards (GASB) standards. The GASB is an independent body that establishes and improves standards of financial accounting and reporting, including the standards that govern the preparation of financial reports of state and government entities. GASB implemented new standards on the calculation of service costs, which could require DIR to change how service costs are calculated. This change could ultimately impact DIR's budgeting cycles and spending.
- DIR receives federal grant money to support certain programs, such as broadband and cybersecurity, within the scope of the agencies. These federal grants require DIR's agreement to federal terms and conditions, which, among other things, establish specific oversight protocol. These administratively created oversight processes or amendments to them may impact DIR's key functions as well as the services that we provide to support state agencies.

Cybersecurity Necessities

Cybersecurity is a priority and focus for DIR. As security protocols and requirements change at the federal and state level and organizations tasked with developing standards and best practices for the field address new concerns and developments, DIR's key functions may be significantly impacted. Ways in which this could occur include:

- If the federal or state governments were to ban the use of certain technologies due to cybersecurity risks, DIR may be required to create an internal or external policy addressing prohibited technologies. In certain cases, DIR would need to implement and enforce policies to stop the use of prohibited technologies. This would also require DIR to find alternatives to accomplish the task previously addressed by the prohibited technology, which would require staff resources, including employee time to research, negotiate, and implement any alternative, and funding to procure

the alternative. This could certainly impact all DIR key functions as it could restrict employee time spent upon other initiatives and programs at DIR.

- If the federal government leveraged additional restrictions on IT supply chains, this stricter federal oversight would require DIR to adhere to the new regulations and potentially limit the vendors and contractors with which DIR could contract. In addition, requirements to manufacture certain technology in the United States could disrupt DIR procurements for the technology and result in higher costs as fewer vendors would be eligible to provide the product or service, reducing competition and the state's negotiating stance. Given DIR's role in delivering technology solutions to state and local government entities, such restrictions would certainly impact DIR's key IT Procurement and Contracting function.
- If cyber threat actors leveraged advances in AI, this could pose significant challenges to DIR's protection of state agency data assets, including state networks and systems, as bad actors could use AI to develop more sophisticated cyber threats, such as more realistic phishing emails and previously undetectable malware. These developments would impact DIR's key function of cybersecurity as DIR is statutorily charged with providing network security services to state agencies that are at the Network Security Operations Center (NSOC),⁴² establishing cybersecurity policy and best practices for the state,⁴³ certifying cybersecurity trainings for completion by state agencies and local governments,⁴⁴ and assisting with cybersecurity incident response throughout the state.⁴⁵

Supply Chain

DIR's Communications Technology Services function empowers Texans to communicate with government by providing a secure statewide network for data, voice, video, and internet. In the early days of the pandemic, DIR observed and was impacted by supply chain issues, resulting in significant delays in the production and delivery of relevant hardware. These supply chain issues for network and IT equipment persist even now with delays in the delivery of certain needed equipment, but so far have had no impact on services through DIR.

h) Overall, how does the agency measure its effectiveness in carrying out its objectives?

Providing excellent customer service is at the heart of DIR's mission, program objectives, and

⁴² [Gov't Code § 2059.051](#); *see also* [Gov't Code § 2059.102](#).

⁴³ [Gov't Code § 2054.0591](#).

⁴⁴ [Gov't Code § 2054.519](#).

⁴⁵ [Gov't Code Chapter 2054, Subchapter N-2](#); Gov't Code Chapter 2059, [Subchapters C, E](#); *see also* [Gov't Code § 2054.0592](#).

core values. DIR's varied stakeholders and customers come from all levels of government, including state agencies, institutions of higher education, judicial organizations, local government entities, school districts, quasi-government organizations, and public entities outside of Texas. DIR measures its effectiveness through various methods across the agency programs, including:

- Customer service-oriented performance measures reported to the Legislative Budget Board;
- Customer and program-specific surveys;
- Performance scorecards and service level agreements;
- Governance groups and advisory committees, including the Customer Advisory Committee;
- Employee performance evaluations; and
- Customer experience strategy and the Voice of the Customer.

Customer Service-Oriented Performance Measures Reported to the Legislative Budget Board

As part of DIR's performance measures reported to the Legislative Budget Board (detailed in Exhibit 2), the performance measures relate specifically to DIR's customer service and meeting of its objectives.

Customer and Program-Specific Surveys

[Chapter 2114 of the Government Code](#) requires state agencies to submit a Report on Customer Service to the Office of the Governor and Legislative Budget Board by June 1 of each even-numbered calendar year.⁴⁶ To satisfy this report, DIR conducts a biennial customer satisfaction survey to all recorded customer entities, which totaled 2,809 contacted entities in 2022. For continuous and updated feedback on DIR's programs and services, DIR also includes this same customer satisfaction survey in every monthly customer newsletter that it sends to over 6,000 contacts.

Each January, the Shared Technology Services program measures customer satisfaction for the previous calendar year. A third-party vendor conducts a comprehensive survey and provides the results to DIR and participating customers. This survey covers all topics required under the Shared Technology Services agreement as well as additional areas of interest. In addition to the annual program surveys, Shared Technology Services customers complete a monthly balanced scorecard, providing feedback to DIR on service provider performance.

Since 2021, the Chief Procurement Office has annually surveyed DIR customers about their familiarity with program offerings, types of offerings, staff knowledge, and customer service.

DIR regularly surveys customers of the Capitol Complex Telephone System (CCTS) and Texas Agency Network (TEX-AN) to determine their satisfaction with DIR's telecommunications

⁴⁶ [Gov't Code Chapter 2114](#).

services. During routine work activities, DIR exchanges emails with customers containing a link to a short survey inviting the customer to express their level of satisfaction with any provided services.

Texas.gov offers its users an opportunity for feedback via two optional surveys to uncover potential areas of the site or services that require corrective action, identify other potential improvement opportunities, and measure overall user satisfaction. These surveys aim to gather, analyze, and measure users' overall satisfaction with the service and performance of the Texas.gov portal and Texas.gov-hosted applications. Upon completion of an online Texas.gov service transaction, users have the option of completing a satisfaction survey. Topics covered in the survey include how the user heard about the online service, how satisfied the user was with their experience, and if the user has any suggestions for improvement. The Texas.gov program also provides a link to the Texas.gov Portal Survey on the Texas.gov website for users to provide feedback at any time.

Performance Scorecards and Service Level Agreements

In addition to the annual program surveys, Shared Technology Services customers complete a monthly scorecard, providing feedback to DIR on service provider performance. Customer rating of service provider performance for FY22 averaged 95 percent satisfaction, with 100 percent satisfaction ratings in May and August 2022, and May 2023.

Service level agreements track compliance with agreed-upon service metrics between DIR and service providers across the Shared Technology Services program. Service level agreement performances are published each month.

Governance Groups and Advisory Committees

DIR receives input and guidance from advisory committees to ensure that customer interests are considered, and business objective improvements are implemented. Groups that provide DIR feedback include the Customer Advisory Committee,⁴⁷ the Data Management Advisory Committee,⁴⁸ the owner-operator governance model of the Shared Technology Services program, the Statewide Information Security Advisory Council, the Texas Cybersecurity Council,⁴⁹ the Security Solutions Group, and the State Strategic Planning Advisory Committee.⁵⁰

- The **Customer Advisory Committee**⁵¹ provides a forum for customer input on their agency's business needs and strategies related to services and programs offered by DIR.

⁴⁷ [Gov't Code § 2054.0331](#); see also [1 Tex. Admin. Code § 201.5\(b\)](#).

⁴⁸ [Gov't Code § 2054.0332](#).

⁴⁹ [Gov't Code § 2054.512](#).

⁵⁰ [Gov't Code § 2054.091\(d\)](#).

⁵¹ [Gov't Code § 2054.0331](#); see also [1 Tex. Admin. Code § 201.5\(b\)](#).

- The **Data Management Advisory Committee**⁵² advises the state Chief Data Officer on the strategic direction for data management practices and policies, in addition to establishing statewide data ethics, principles, goals, strategies, standards, and architecture. The Data Management Advisory Committee provides guidance and recommendations on governing and managing state agency data and data management systems, including recommendations for assisting Data Management Officers. The Data Management Advisory Committee establishes performance objectives for state agencies from Texas' data-driven policy goals.
- The **owner-operator governance model** of the Shared Technology Services program allows customers to work directly with all service providers to resolve local operational issues specific to the customer. Both customers and service providers participate in committees to address enterprise matters. Owner-operator governance functions on three levels: DIR customer meetings, partner group meetings, and enterprise governance meetings. The governance structure includes a customer-chaired Business Executive Leadership Committee and several IT Leadership Committee and Solution Groups.
- The **Statewide Information Security Advisory Council** provides guidance for protecting and improving the confidentiality, integrity, and security of Texas government information assets and technology. The committee also utilizes subcommittees as needed relating to information security policy and risk management.
- The **Texas Cybersecurity Council**⁵³ provides enduring partnerships between Texas private industry and public sector organizations. These partnerships ensure that critical infrastructure and sensitive information are protected, cultivate an exemplary cybersecurity workforce to protect technology resources from increasing threats, and develop strategies and solutions that ensure that Texas continues to lead in areas of cybersecurity at a national level.
- The **Security Solutions Group** promotes effective security and performance in DIR's Shared Technology Services program in alignment with [1 Texas Administrative Code Chapter 202](#).⁵⁴ The Security Solutions Group oversees enterprise security-related activities, monitors security performance trends, and addresses enterprise security-related issues and gaps.

⁵² [Gov't Code § 2054.0332](#).

⁵³ [Gov't Code § 2054.512](#).

⁵⁴ [1 Tex. Admin. Code Chapter 202](#).

- The **State Strategic Plan Advisory Committee**⁵⁵ provides insight into statewide technological trends and forecasts and advises DIR on the development of the State Strategic Plan for Information Resources Management.

Employee Performance Evaluations

DIR uses employee performance evaluations to measure and assess an employee's day-to-day contributions to the overall goals and objectives of the agency. The performance review process is used to acknowledge an employee's contributions and to offer constructive suggestions for improvement when necessary. Every DIR employee is evaluated on the DIR core objectives of innovation, leadership, ethics, accountability, and delivery (ILEAD).

Customer Experience Strategy and the Voice of the Customer

In FY23, DIR initiated the agency-wide customer experience strategy to work across agency divisions and collaborate on optimizing interactions with DIR stakeholders. The Voice of the Customer identifies the ways that DIR collects customer feedback as outlined in the chart below. As part of the overall customer experience strategy, this feedback informs DIR's compliance, process improvement, and accomplishment of strategic objectives.

Figure 3 Methods of Customer Feedback - Voice of the Customer

Method, Tool,	Customers	Intentions	Frequency	What is done with the feedback?
Data Management				
Texas Open Data Portal (ODP) Survey	Texas ODP users	Gather feedback from public data consumers on their experience using the ODP	Once (possible annual)	ODP Admin shared with Office of Chief Data Office (OCDO), used to identify user challenges
E-Records Conference Surveys	Records management professionals	Gather feedback from attendees	Annual	Used to improve offerings for following year, suggest additional topics
DIR Discover Conference Survey	Data management professionals	Gather feedback from attendees	Annual	Used to improve offerings for following year, suggest additional topics
Texas Data Literacy Program (TDLP) Course Evaluations	Participants of the TDLP eLearning courses	Gather feedback on the effectiveness of data literacy course to aid in the development of future courses	Once (per course)	Course evaluation results are reviewed and presented to stakeholders (DMAC and Data Literacy Workgroup members). Discussions with those two groups lead to priorities for improvements.

⁵⁵ [Gov't Code § 2054.091\(d\)](#); see also [1 Tex. Admin. Code § 201.5\(a\)](#).

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
Data Literacy Assessment Survey	Data Management Officers (DMO) and/or their designees; members of the Texas Enterprise Information Management (TEIM) networking group	Determine the potential audience for data literacy education efforts and the priority of data literacy topics to address the new TDLP	Annual	Responses help prioritize and ensure TDLP offerings remain relevant for advancing data management in Texas
Data Management Advisory Committee (DMAC) Input Survey	DMOs and/or their designees	Determine topics to include on future DMAC meeting agendas	Once	Information collected on the survey helps determine topics to include on future meeting agendas
TEIM Input Survey	Members of the TEIM networking group	Determine topics to include on future TEIM meeting agendas	Once	Information collected on the survey helps determine topics to include on future meeting agendas
Open Data Portal/Closed Data Portal (ODP/CDP) Customer Check-in Emails	Agency and institution of higher education representatives involved in open data publishing on ODP or data sharing on CDP	Assess where customer is in the publishing process and if any support is needed	As needed but at least monthly	Feedback retained by ODP Administrator to improve support to customers; May include ODP/CDP support tickets for enhancements or troubleshooting
ODP/CDP Customer Meetings	Agency and institutions of higher education representatives involved in open data publishing on ODP or data sharing on CDP	Provide targeted training and troubleshooting	Onboarding; as needed	Feedback retained by ODP Administrator to improve future presentations and support to customers; may include ODP/CDP support tickets for enhancements or trouble shooting. ODP/CDP "wish list" maintained by ODP Admin for discussions with vendor on improvements.
ODP/CDP presentations	Agency and institution of higher education representatives interested in open data publishing on ODP or data sharing on CDP	Provide information to prospective customers	As requested	Feedback retained by ODP Administrator to improve future presentations and support to customers
Collaborative Email Addresses: OCDO@dir.texas.gov;	Data Management Officers and/or their designees; agency and institution of	Provide a method of asking questions and providing feedback	As needed	Feedback used by OCDO to improve services

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
txopendataportal@dir.texas.gov	higher education representatives involved or interested in open data publishing on ODP or data sharing on CDP or the TDLP			
Cybersecurity				
Information Security Forum (ISF) Survey	Attendees and exhibitors	Get feedback on the conference	Once	Feedback is incorporated into lessons learned document to improve future conferences
Statewide Incident Response Working Group (SWIRG)	DIR, Texas Military Department (TMD), Texas Division of Emergency Management (TDEM), Texas Department of Public Safety (DPS), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), private vendors, other state and federal partners	Coordinate statewide response to significant cybersecurity incident	Quarterly	Feedback is recorded and incorporated into the state's information resources (IR) plan with a goal of simplifying and gaining a better understanding of partner capabilities and resources
Statewide Information and Security Advisory Committee (SISAC)	SISAC members	Members discuss best practices and make recommendations to DIR	Monthly	Recommendations to DIR are considered for more effective security operations
SISAC Communications Subcommittee	Subcommittee members	Helps provide communication to agencies about progress of the DIR statewide security program and associated events and helps evaluate feedback from agencies	As needed	Information provided is shared with agencies and agency feedback is incorporated into planning activities
SISAC Solutions Subcommittee	Subcommittee members	Evaluates solutions to common problems and shares best practices among agencies	As needed	Recommendations to DIR are considered for more effective security operations

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
SISAC Risk Assessment Subcommittee	Subcommittee members	Helps define the state's risk assessment methodology for the consistent evaluation of risk within state agencies	As needed	Recommendations to DIR are considered and incorporated into planning activities
Texas Cybersecurity Council	Council members; selected public and private sector representatives	Develops partnerships, strategies, and solutions to protect critical infrastructure, develop the cybersecurity workforce, and support Texas' cybersecurity posture	Bi-monthly	Recommendations are shared with DIR and/or included in an annual report to the Legislature
Texas Information Sharing and Analysis Organization (TX-ISAO) Partners	Partner members	Contribute to and support the TX-ISAO	As needed	Changes are shared with DIR and incorporated into TX-ISAO operations/ services, as needed
TX-ISAO Threat Reports	TX-ISAO members	Receive cyber threats	Ongoing	Submissions are forwarded to the TX-ISAO partners for possible research and dissemination
Communications Technology Services (CTS) / Capitol Complex Telephone System (CCTS)				
Communications Technology Services /Capitol Complex Telephone System (CTS/CCTS) Survey	CTS/CCTS	Gauge customer satisfaction with CTS/CCTS from the ordering process, installation of services, and day-to-day repair of services	When email is sent from orders or CCTS, a link is included on the DIR employee's email signature for customers to access survey	Legislative Budget Board (LBB) measure; also, will reach out to customers who provide their information so issue can be addressed and/or resolved
Shared Technology Services (STS)				
Shared Technology Services (STS) Annual Customer Satisfaction Survey: distributed via email by contracted vendor managed by Multi-sourcing Services Integrator (MSI)	STS customers: business executives, IT staff, and DIR staff.	LBB measurement for customer satisfaction	Annually	Information is provided to the service component providers (SCPs) for process improvement. Also shared with the members of DIR's governing board, the Business Executive Leadership Committee, and the IT Leadership Committee.
Customer Scorecard: available through the STS portal	STS customers	Customers rate the service performance according to each program and provide	Monthly	Ratings of 1 or 2 automatically generate a service request assigned to the (MSI) Customer

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
		subjective commentary, including service request examples where applicable		Relationship Manager (CRM) for resolution tracking. The MSI CRM will update the service request with next steps and status. When SCP action is required, the MSI CRM will assign a task from the primary service request to accomplish the needed action. The customer will receive follow up on the item during scheduled meetings with the assigned MSI CRM.
Constituent Help Desk Customer Satisfaction Survey: point-of-service surveys will be offered based on live chats with constituent help desk agents.	Constituents with access to the Texas.gov portal	Measures the average scores of the customer satisfaction surveys taken on a random statistical sample of customers that had a service contact with the SCP during the measurement window	Conducted daily, to at least every fifth contact. The service level compliance report is updated weekly.	The customer satisfaction results are shared with SCPs for additional training and continuous improvement
Service Desk Customer Satisfaction Survey: sent out daily to contacts based on 20% of resolved incidents and completed requests.	STS customers	Measures the average scores of the customer satisfaction surveys taken on a random statistical sample of customers that had a service contact with the SCP during the measurement window	The service level compliance report is updated daily	The customer satisfaction results are shared with SCPs for additional training and continuous improvement
Ad Hoc Feedback: STS Portal Request	STS customers	To provide customers with an outlet through which to submit feedback on the STS	As needed	The feedback is shared with SCPs for additional training and continuous improvement
Procurement and Contracting				
Chief Procurement Office (CPO) 2021 Survey	DIR vendors	Gather feedback from existing DIR vendor community on processes, DIR staff, etc.	Once, but may repeat in future	CPO leadership reviews results
CPO 2021 and 2023 Survey	DIR customers	Gather feedback from customer community on DIR's programs	Have completed two; ideally biennially.	Program Data Analysis and Reporting team analyzes results; CPO leadership reviews results

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
AskDIR	Customers and vendors	Answer customer questions on any procurement or contract-related inquires	Ongoing	Handled from the AskDIR email box. Each one is handled on a case-by-case basis and is monitored for completion when task is done.
Trainings: in-person and online	DIR customers; part of Certified Texas Contract Developer/Certified Texas Contract Manager/Business Technology Platform (CTCD/CTCM/BTP) training through the Comptroller.	Train customers and build relationships with DIR's customer base. Many customers provide input through questions they ask during the trainings.	As needed; and per the Comptroller's scheduled trainings.	Listen to customers questions on how they feel about utilizing DIR's programs and services
Townhall Webinars	DIR vendors and customers	Provide bulk-purchase input and needs	As needed/ ongoing	Information gained directly from vendors and customers to determine bulk purchase plans for DIR and DIR customers
Public Information Requests	External general public	Provide requested information for those who file public information requests seeking procurement or contract information	As needed/ ongoing	Communicated to legal and CPO leadership on status of what is being requested
Technology Guidance and Innovation				
AskDIR	Customers and vendors	Answer customer questions on any procurement or contract-related inquires	Ongoing	Handled from the AskDIR email box. Each one is handled on a case-by-case basis and is monitored for completion when task is done.
State Strategic Plan (SSP) Advisory Committee	Customers, private industry, and constituent representation	Strategic direction and vision for SSP	Multiple meetings held in odd-numbered years for preparation of the SSP	Incorporate feedback for strategic direction. Establishes the strategic goals for technology in the state.
Customer Groups: Customer Advisory Committee (CAC), Business Executive Leadership Committee (BELC), Information	Feedback	Customer feedback mechanism	Monthly	Incorporate feedback for strategic direction and operational related items

Method, Tool, Platform	Customers	Intentions	Frequency	What is done with the feedback?
Technology Leadership Committee (ITLC), Shared Technology Services (STS) Governance Bodies				
Agency Strategic Plan	Has a specific customer satisfaction requirement. PDO distributes the survey, and it is incorporated into the plan.	Receive feedback from customers	Bi-annually	Shared with DIR's program areas for continuous improvement.
Information Resources Deployment Review (IRDR) Reporting	Gauging the current technology environment, compliance, and progress towards strategic goals; collect feedback on customer satisfaction.	Receive feedback from customers	Bi-annually	Measures an agency's progress against the State Strategic Plan (SSP). Confirms that the agency is complying with the state's technology-related statutes, rules, and standards. Examines how each information resource deployment has supported the agency's mission, goals, and objectives.
Quality Assurance Team (QAT): Oversight Body	Not a significant amount of feedback through this forum. Talk to other QAT members and their input is incorporated in the feedback provided to the Legislature. For QAT purposes, the Legislature and agencies' executive leadership are the customers, and not the agencies' IT staff.	Provide oversight of large projects; provide feedback to legislative and agency leadership	Monthly	Provide feedback to legislative and agency leadership
AskDIR	Customers and vendors	Answer customer questions on any procurement or contract-related inquiries	Ongoing	Handled from the AskDIR email box. Each one is handled on a case-by-case basis and is monitored for completion when task is done.

Method, Tool,	Customers	Intentions	Frequency	What is done with the feedback?
Annual Customer Satisfaction Survey	DIR customers	Required by statute. Assess DIR's performance.	Annually	Shared with DIR's program areas for continuous improvement. Shared with the members of DIR's governing board, the Business Executive Leadership Committee, and the IT Leadership Committee.
Agency Administration				
Customer Advisory Committee (CAC)	DIR customers	Required by statute. Opportunity for customers to provide input on programs.	Quarterly	Incorporate feedback for strategic direction and operational related items

In the following chart, provide information regarding your agency's key performance measures, including outcome, input, efficiency, and explanatory measures. Please provide both key and non-key performance measures set by the Legislative Budget Board as well as any other performance measures or indicators tracked by the agency. (Numbers are for reference in Section VII.)

Texas Department of Information Resources

Exhibit 2: Performance Measures – Fiscal Year 2022

Key Performance Measures	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
Number of Technology Solutions and Services Reviewed	The number of technology solutions and services reviewed is counted.	60	59	98.33%
Number of Agencies Participating in Pilot Projects for Enterprise Solutions	The number of agency participations in each pilot of enterprise solutions and services is counted. A single agency participating in more than one pilot will be counted twice or more, based on the number of pilots in which the agency is participating.	10	14	140%
Percent of Monthly Minimum Service Level Targets Achieved	The initial Critical Service Level Matrix of thirty (30) critical service levels is defined in the Data Center Services (DCS) Agreement. The DCS contract library contains documentation of: the matrix, modifications to the designation of a particular measure as "critical," and changes to the financial credits associated with not meeting a particular "critical" measure. The percentage is calculated by using the following formula: (number of monthly critical minimum service levels met	95%	98.95%	104.16%

Key Performance Measures	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
	during the period) divided by (total number of monthly critical service levels measured during the period) times 100%.			
Percent of Customers Satisfied with Shared Technology Services Contract Management	The percentage is calculated using the following formula: (respondents rating the DCS contract management job DIR is doing as good or excellent) divided by (all respondents giving a rating) times 100%.	85%	73%	85.88% ⁵⁶
Percent of Customers Satisfied with CCTS	Customer satisfaction results are entered into a database and are based on the web survey responses from CCTS users. Results are averaged based upon the number of survey responses.	90%	90.24%	100.27%
Percent Customers Satisfied with TEX-AN	Customer satisfaction results are entered into a database and are based on the web survey responses from TEX-AN users. Results are averaged based upon the number of survey responses	90%	91.18%	101.31%
Total Savings through DIR Cooperative Contracts	Cost savings will be calculated by taking the sum of all eligible sales differences between the MSRP and final sales price.	\$250,000,000	\$394,972,082.50	157.99%
Number of Transactions Conducted through the Portal	Each online payment transaction is captured by the state electronic internet portal, Texas.gov's payment service and routed through the banking and credit card systems.	40,000,000	57,445,552	143.61%
Percent of Agencies' Critical Telecom Network Security Vulnerabilities Reduced	Number of critical security vulnerabilities remediated voluntarily reported divided by total number of critical security vulnerabilities identified.	50%	55.46%	110.92%
Percentage of State Agencies that participate in DIR-Provided Security Training Offerings	Manual count of all agencies and institution of higher education represented at DIR cyber security training offerings divided by the total numbers of agencies and institutions of higher education.	65%	87%	133.85%
Number of State Agency Security Assessments Performed	Manual count of individual completed security assessments	40	44	110%

⁵⁶ The numbers that will be reported for FY23, using identical calculations, show satisfaction increased to 80% which is 94.1% of goal. During the 88th session, the LBB changed this performance measure seeking more consistent and accurate data by using DIR's monthly customer surveys as the measurement rather than an annual, point-in-time survey.

These measures are an estimate because FY22 Non-Key Performance Measures are not due until the Itemized Operating Budget is submitted in December 2023.

Non-Key Performance	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
Percentage of DIR Recommendations Enacted	The number of recommendations enacted through legislation is divided by the total number of recommendations made in legislative reports. Some recommendations may be modified by the legislature before adoption but are counted in the totals. Recommendations made and legislation enacted are counted manually.	75% (Biennial)	NA (Measure is only reported for odd numbered fiscal years)	NA
Percentage of Attendees Favorably Rating Education Events	The total number of favorable ratings is divided by the total number of evaluation responses received for the event.	90%	96%	107%
Percentage of IRMs Meeting CE Requirements	Number is determined by analyzing reports submitted by IRMs and determining which IRMs are meeting CE requirements. Analysts manually compare reports submitted with the requirements to determine if IRMs are meeting the requirements. The number of agencies determined to be in compliance is then divided by the total number of agencies for which DIR CE rule applies.	85%	95%	112%
Average Cost Per Statewide IR Recommendation Produced	The total time spent developing recommendations is divided by the total number of recommendations, then multiplied by an average hourly rate, which includes average hourly staff salary, benefits, and overhead.	2,250	NA (Measure is only reported for odd numbered fiscal years)	NA
Number of Statewide IR Recommendations Produced	The number of recommendations in the Biennial Performance Report on Information Resources Management and other legislative reports is counted.	6	NA (Measure is only reported for odd numbered fiscal years)	NA
Number of Briefings, Workgroups, and Focus Groups Conducted by DIR	Manual count of hosted briefings, workgroups, and focus groups conducted by DIR	50	275	550%
Number of Education Programs Produced	Manual count of all educational events sponsored by DIR	50	51	102%
Number of Rules, Guidelines and Standards Produced	Manual count of rules, guidelines, and standards produced during the quarter	10	5	50%

Non-Key Performance Measures	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
Number of State Agency Personnel Trained on Framework & Project Delivery	Manual count of all state personnel attending framework and project delivery educational events	200	286	143%
Percentage of Eligible Texas Local Government Entities Using DIR Services	The number of eligible local government entities executing transactions divided by the total number of eligible local government entities. Eligible entities are defined as political subdivisions and other local government entities authorized to use DIR contracts by Texas Government Code Chapters 2054, 2157, and 2170. This excludes Assistance Organizations as defined by Texas Government Code Section 2175.001 and Public Entities outside of Texas as defined by Texas Government Code Section 2054.0565	50%	60%	120%
Average Cost Recovery Rate for Cooperative Contracts	Divide the total administrative fees collected by gross sales to determine the average cost recovery rate.	0.67%	0.7%	104%
Total DIR Gross Sales	Sum total of all sales from IT commodity and service contracts (cooperative contracts).	\$2,200,000,000	\$3,050,000,000	139%
Number of Exemptions Requested for IT Commodities and Services	Manual count	650	400	62%
Number of State Agencies Participating in Bulk Purchase Agreements	DIR will negotiate bulk purchase agreements. Participating agencies submit to DIR purchase orders issued under bulk purchase agreements. DIR will accumulate purchase orders to determine the number of participating agencies. DIR will report to LBB the number of agencies participating in each bulk purchase agreement for the fiscal year	40	20	50%
Percentage of Visitors Satisfied with Texas.Gov	Texas.gov will provide the customer satisfaction survey instrument on each application. Results will be collected online and analyzed quarterly for trends. The number of satisfied survey respondents divided by total survey responses.	95%	85%	89%
Texas.Gov Collections Deposited into the General Revenue Fund	Measure reflects the balance of revenues collected from Texas.gov transactions and deposited to the Statewide Network Applications	\$31,000,000	\$35,000,000	113%

Non-Key Performance Measures	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
	Account which are required to be transferred to the General Revenue Fund pursuant to Article IX, Payments to the Department of Information Resources, of the General Appropriations Act in effect for the fiscal year in which the revenues were collected. Per the Article IX provision, amounts in excess of allowable balances collected in a fiscal year will be transferred to the General Revenue Fund. Refer to the Article IX provision for the calculation of the amount to be transferred to the General Revenue; the provision is subject to revision each biennium.			
Number of Services Available through the Portal	New services are brought online through various governance mechanisms. The number and list of services are tracked by the vendor.	1,000	855	85.5%
Percentage of CCTS Complaints/Problems Resolved in 8 Working Hours or Less	The CCTS Manager uses the CCTS Trouble Ticket Management system report on Trouble Tickets by Technician to manually count from the report of the entries of Trouble Tickets that took less than 8 hours. This number is subtracted from the total number of Trouble Tickets which is calculated by the report. The count of those that took less than 8 hours is given as a percent of the total number of Trouble Tickets completed for the reporting period obtained.	97%	91%	94%
CCTS Trouble Tickets As a Percentage of Lines in Service	The CCTS manager will divide the number of Trouble tickets completed for the reporting period by the average number of stations on the system.	2%	0.43%	22%
Average Price Per Intrastate Minute on TEX-AN	Total dollar amounts divided by total of minutes for intrastate calls	0.02	0.02337	117%
Average Price Per Interstate Minute on TEX-AN	Total dollar amounts divided by total of minutes for interstate calls	0.02	0.02458	123%
Average Price Per Toll-Free Minute on TEX-AN	Total dollar amounts divided by total of minutes for Toll-Free calls	0.02	0.07609	380%
TEX-AN Trouble Tickets As A Percentage of Circuits	The number of trouble tickets reported is divided by the number of circuits billed.	6%	6.20%	103%

Non-Key Performance Measures	Calculation (if applicable)	FY 2022 Target	FY 2022 Actual Performance	FY 2022 % of Annual Target
Average Price of Data Services	The number of circuits are obtained from the total for all customers from the telemanagement system for the reporting period. The dollar amount billed is divided by the corresponding total count of circuits. The port charge is added, and the total multiplied by two.	\$820.00	\$830.13	101%
Average Cost of Security Controlled Penetration Tests	The vendor's average value of a security-controlled penetration test.	\$21,768	\$9,873	45%
Number of Security Controlled Penetration Tests	Manual count of individual security-controlled penetration tests including follow-up or additional tests of the same state entity.	50	66	132%

- i) Please list all key datasets your agency maintains and briefly explain why the agency collects them and what the data is used for. Is the agency required by any other state or federal law to collect or maintain these datasets? Please note any “high-value data” the agency collects as defined by Texas Government Code Section 2054.1265.57 In addition, please note whether your agency posts those high-value datasets on publicly available websites as required by statute, and in what format.

Texas Department of Information Resources

Exhibit 3: Key Datasets

Dataset	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
OCDO-1	IHE Agency Tracking	This spreadsheet tracks agency and IHE Data Management Officers and Open Data Portal (ODP) contacts for onboarding purposes and to provide additional support to agencies preparing to publish on the ODP. The dataset contains the names, titles, email addresses, and organization of designated Data Management Officers, ODP contacts, and secondary contacts. The dataset also includes information on when DMO resource information was provided, and status of ODP publishing.	Agency	Not public	N
OCDO-2	DMO and ODP Contacts	This spreadsheet provides Data Management Officer (DMO) and ODP contacts for each agency for collaboration opportunities, including invitations to the Data Management Advisory Committee (DMAC). The dataset contains the names,	Agency	Not public, but shared with DMOs and ODP contacts for education and collaboration.	N

⁵⁷ [Gov't Code § 2054.1265.](#)

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
		email addresses, and organization of designated Data Management Officers, ODP contacts, and secondary contacts.			
OCDO-3	Texas Domain Tracking	This tracking spreadsheet assists the OCDO in forecasting potential ODP and Closed Data Portal (CDP) Growth. It measures the number of unique role user logins per month. Important to track because of contracted user caps with tiered pricing.	Agency	Not public but posted internally.	N
OCDO-4	ODP SLA Reports	Tyler Technologies provides service level agreement (SLA) data to the ODP Administrator each month to compare to SLA thresholds included in ODP contract.	Agency, Tyler Technologies	Not public but posted internally.	N
OCDO-5	ODP Site Statistics	Monthly utilization statistics on ODP usage including # of assets, downloads, and visits. This data is reported to Data Management Advisory Committee, Open Data Portal User Group, and DIR Board.	Agency	Not public but posted internally.	N
OCDO-6	TSDEC	Agencies and institutions of higher education that are participating in the Texas Statewide Data Exchange Compact (TSDEC) data sharing agreement.	Agency	Not public but posted internally.	N
OCDO-7	ODP Terms and Conditions	Agencies and institutions of higher education that have agreed to the Open Data Portal Terms and Conditions. The dataset contains links to the interagency contract documents.	Agency	Not public but posted internally.	N
OCDO-8	OCDO KPI Dashboard	Provides metric tracking of internal key performance	Agency	Not public but posted internally.	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
		indicators for the OCDO. Dataset contains aggregate numbers only.			
OCDO-9	HR KPI Dashboard	Provides metric tracking of internal key performance indicators for People and Culture Office.	Agency	Not public but posted internally.	Y
TDLP-1	Registration Documentation	Texas Data Literacy Program registration and participation data. Collecting and monitoring this data helps ensure judicious distribution of learning management system licenses purchased by DIR, as well as to monitor state agency and institutions of higher education participation.	Agency	Not public but posted internally.	N
TDLP-2	eLearning Report Master	Texas Data Literacy Program eLearning course participation data. Collecting and monitoring this data helps to track course completion by participants. Participants who complete all courses in the foundation track of data literacy courses will receive a certificate of completion. This data also includes individual course evaluation responses that are used to make improvements to the Texas Data Literacy Program courses.	Agency	Not public but posted internally.	N
ODP-1	Bid Book Spreadsheet 2016	2016 HUB bid fair agency solicitations.	Agency	https://data.texas.gov/dataset/Bid-Book-Spreadsheet-2016/daek-f7x4	N
ODP-2	Official DIR Cooperative Contract Sales Data Fiscal 2010 to Present	Optimized version of DIR Cooperative Contract Sales Data Fiscal 2010 To Present. This dataset was made active September 07, 2018,	Agency	https://data.texas.gov/dataset/OFFICIAL-DIR-Cooperative-Contract-Sales-	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
		and includes data going back to 2010.		Data-Fisca/w64c-ndf7	
ODP-3	Bid Book Spreadsheet 2018	2018 HUB bid fair agency solicitations.	Agency	https://data.texas.gov/Government-and-Taxes/Bid-Book-Spreadsheet-2018/9apk-jjpi	N
ODP-4	Bid Book Spreadsheet 2020	2020 HUB bid fair agency solicitations.	Agency	https://data.texas.gov/Government-and-Taxes/Bid-Book-Spreadsheet-2020/uk2f-keq4	N
ODP-5	Bid Book Spreadsheet 2017	2017 HUB bid fair agency solicitations.	Agency	https://data.texas.gov/Business-and-Economy/Bid-Book-Spreadsheet-2017/qwhy-c2kk	N
ODP-6	2023 SRWDBTSSBF Bid Book Spreadsheet	Bid Book Spreadsheet for Senator Royce West Doing Business Texas Style Spot Bid Portal FY2023	Agency	https://data.texas.gov/dataset/2023-SRWDBTSSBF-Bid-Book-Spreadsheet/89zk-ru79	N
ODP-7	Bid Book Spreadsheet 2019	2019 HUB bid fair agency solicitations.	Agency	https://data.texas.gov/Government-and-Taxes/Bid-Book-Spreadsheet-2019/4qh5-bvt7	N
ODP-8	2022 SRWDBTSSBF Bid Book Spreadsheet	Bid Book Spreadsheet for Senator Royce West Doing Business Texas Style Spot Bid Portal FY2022	Agency	https://data.texas.gov/dataset/2022-SRWDBTSSBF-Bid-Book-Spreadsheet/fey9-gcem	N
ODP-9	Bid Book Spreadsheet 2021	2021 Senator Royce West Doing Business Texas Style Spot Bid Fair (SRWDBTSSBF) Submissions	Agency	https://data.texas.gov/dataset/Bid-Book-Spreadsheet-2021/nutf-4rvq	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
ODP-10	OFFICIAL - Customer list - Cooperative Contracts - Texas Department of Information Resources - - Data from vendor sales reports	This data is a listing of customers reported from the monthly vendor sales reports.	Agency	https://data.texas.gov/dataset/OFFICIAL-Customer-list-Cooperative-Contracts-Texas/4v6c-qfkr	N
ODP-11	Official DIR Current Active Cooperative Contracts	This lists the active contracts currently offered through DIR's Cooperative Contract program.	Agency	https://data.texas.gov/dataset/OFFICIAL-DIR-Current-Active-Cooperative-Contracts/vipt-h4ye	N
ODP-12	HMSDC 2020 Bid Fair Spreadsheet	2020 Houston Minority Supplier Development Council Spot Bid Fair Post Award Summary for State Agencies and IHEs.	Agency	https://data.texas.gov/dataset/HMSDC-2020-Bid-Fair-Spreadsheet/dxdw-hs8h	N
ODP-13	HMSDC 2021 Bid Fair Spreadsheet	2021 Houston Minority Supplier Development Council Spot Bid Fair Post Award Summary for State Agencies and IHEs.	Agency	https://data.texas.gov/dataset/HMSDC-2021-Bid-Fair-Spreadsheet/2bk4-b5yq	N
ODP-14	2022 HMSDC Bid Fair Spreadsheet	2022 Houston Minority Supplier Development Council Spot Bid Fair Post Award Summary for State Agencies and IHEs.	Agency	https://data.texas.gov/dataset/2022-HMSDC-Bid-Fair-Spreadsheet/4fsv-mqtm	N
ODP-15	2017 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2017-SRWDBTSSBF-Post-Award-Summary/vqgi-kzuj	N
ODP-16	2021 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2021-SRWDBTSSBF-Post-Award-Summary/sxt7-uuaj	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
ODP-17	2017 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2017-SRWDBTSSBF-Post-Award-Summary/vqgi-kzuj	N
ODP-18	2019 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/Business-and-Economy/2019-SRWDBTSSBF-Post-Award-Summary/vafe-2xdg	N
ODP-19	2018 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/Government-and-Taxes/2018-SRWDBTSSBF-Post-Award-Summary/sufq-rnri	N
ODP-20	2020 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2020-SRWDBTSSBF-Post-Award-Summary/h3aq-tb43	N
ODP-21	2022 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2022-SRWDBTSSBF-Post-Award-Summary/842z-m2re	N
ODP-22	BPR Alignment	State agency alignment with goals and objectives outlined in the 2020 State Strategic Plan for Information Resources Management as reported in the 2020 Information Resources Deployment Review (IRDR).	Agency	https://data.texas.gov/dataset/BPR-Alignment/8f6m-78bg	N
ODP-23	2023 SRWDBTSSBF Post Award Summary	Senator Royce West Doing Business Texas Style Spot Bid Fair Post Award Summary	Agency	https://data.texas.gov/dataset/2023-SRWDBTSSBF-Post-Award-Summary	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
				Summary/n6zg-kzrz	
ODP-24	2020 HMSDC Post Award Summary	2020 Houston Minority Supplier Development Council Spot Bid Fair Post Award Summary for State Agencies and IHEs.	Agency	https://data.texas.gov/dataset/2020-HMSDC-Post-Award-Summary/7jaj-c3xu	N
ODP-25	Digital Transformation IRDR Data	DIR has established a digital transformation guide to assist agencies with modernizing agency operations and services with respect to electronic data and converting agency information into electronic data.	Agency	https://data.texas.gov/dataset/Digital-Transformation-IRDR-Data/y7wk-dk9k	N
ODP-26	BPR Summary Data	Biennial Performance Report (BPR) summary data for report visualizations. Contains aggregate IRDR responses to select questions.	Agency	https://data.texas.gov/dataset/BPR-Summary-Data/cu3v-5rpi	N
ODP-27	2021 HMSDC Post Award Summary	2021 Houston Minority Supplier Development Council Spot Bid Fair Post Award Summary for State Agencies and IHEs.	Agency	https://data.texas.gov/dataset/2021-HMSDC-Post-Award-Summary/4cyt-s762	N
ODP-28	2021 IT Leadership Survey Trends	Results from the survey sent to state IT leaders. They were asked to identify the technology developments and initiatives that are most important to their organizations.	Agency	https://data.texas.gov/dataset/2021-IT-Leadership-Survey-Trends/39c4-xuns	N
ODP-29	2022 BPR Alignment	This data depicts state agency alignment with 2020 State Strategic Plan for Information Resources Management goals and objectives reported in the 2020 BPR.	Agency	https://data.texas.gov/dataset/2022-BPR-Alignment/cpqa-42ub	N
ODP-30	2022 HMSDC Post Award Summary	2022 Houston Minority Supplier Development Council Spot Bid Fair Post	Agency	https://data.texas.gov/dataset/2022-HMSDC-Post-	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
		Award Summary for State Agencies and IHEs.		Award-Summary/i6sa-ryey	
ODP-31	2022 BPR Goals 4	Goals 1-4	Agency	https://data.texas.gov/dataset/2022-BPR-Goals-4/xmp6-qics	N
ODP-32	2022 BPR Figure 1	Top Security Initiatives for Next Biennium	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-1/qswm-n2zf	N
ODP-33	2022 BPR Figure 7a	Fig. 7: Digital Transformation Maturity	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-7a/nwvs-sq8g	N
ODP-34	2022 BPR Figure 11	Fig. 11: Native Mobile App Capability	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-11/24f2-9h93	N
ODP-35	2022 BPR Figure 14	Fig. 14: Top Barriers to Deploying AI Solutions	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-14/jbdv-82ha	N
ODP-36	2022 BPR Figure 3	Fig. 3: Top Barriers to Cybersecurity	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-3/yrf3-apwi	N
ODP-37	2022 BPR Figure 15	Fig. 15: Use of Emerging Technologies and Tools	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-15/g2i4-jkmi	N
ODP-38	2022 BPR Figure 2	Fig. 2: Security Incident Response	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-2/ycjs-p8i8	N
ODP-39	2022 BPR Figure 4	Fig. 4: Data Management and Governance	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-4/xtc9-9a27	N
ODP-40	2022 BPR Figure 8	Fig. 8: Paperless Processes	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-8/iy6h-2sd3	N
ODP-41	2022 BPR Figure 12	Fig. 12: Top AI Priorities	Agency	https://data.texas.gov/dataset/2022-	N

Dataset Reference Number	Dataset Name	Description of Data	Data Maintained By	Hyperlink (if publicly available)	Legal Prohibition to Disclosure Y/N
				BPR-Figure-12/fhua-i9t8	
ODP-42	2022 BPR Figure 13	Fig. 13: Progress on Emerging Technologies	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-13/udk7-z9zc	N
ODP-43	2022 BPR Figure 10	Fig. 10: Agencies' Ability to Embrace Digital Transformation	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-10/7kae-xrwh	N
ODP-44	2022 BPR Figure 5	Fig. 5: Top Barriers to Data Management and Governance	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-5/sadh-3yix	N
ODP-45	2022 BPR Figure 9	Fig. 9: Online Board Meetings	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-9/y2uj-2mrs	N
ODP-46	2022 BPR Figure 6a	Fig. 6: Data Classification Maturity	Agency	https://data.texas.gov/dataset/2022-BPR-Figure-6a/ydsn-36hq	N

III. History and Major Events

a) Provide a timeline of your agency's history and key events.

1967

The Legislature began efforts to contend with the challenges associated with the management of information resources by creating the Systems Division in the State Auditor's Office to maintain comprehensive and current information on data processing systems in state agencies.

1979

The Legislature created the State Purchasing and General Services Commission to provide support services for state agencies including telecommunications services (among other duties).⁵⁸ The State Auditor's Office Systems Division advised the State Purchasing and General Services Commission on procuring data processing resources and was actively involved in its oversight.⁵⁹

1981

The Legislature established the Automated Information Systems Advisory Council (AISAC) to promote state government's economical and efficient use of automated information systems by adopting policies for state government bodies.⁶⁰ The AISAC adopted policies for the purchase or lease of automated information systems, the computers on which they are automated, and services related to the automation of information systems or the computers on which the systems are automated. In addition to promoting these policies, the enabling legislation authorized the AISAC to review and report to state leadership on certain technology purchase requests made by state agencies. The AISAC notified the State Purchasing and General Services Commission of these requests and created guidelines for long-range planning, common databases, networking, applications, shared software, security, and disaster recovery.

1985

The Legislature retitled the AISAC as the Automated Information and Telecommunications Council (AIRC).⁶¹ Additionally, the Legislature broadened the Council's mandate to include preparing a long-range telecommunications plan and providing technical assistance to state agencies and their staff to support the Legislative Budget Board on requests for appropriations for technology.⁶²

⁵⁸ [Acts 1979, 66th Leg., R.S., ch. 773 \(H.B. 1673\), 1979 Tex. Gen. Laws 1908.](#)

⁵⁹ [Acts 1981, 67th Leg., R.S., ch. 737 \(H.B. 1463\), 1981 Tex. Gen. Laws 2701.](#)

⁶⁰ *Id.* See also [Acts 1981, 67th Leg., 1st C.S., ch. 16 \(H.B. 113\), 1981 Tex. Gen. Laws 185.](#)

⁶¹ [Acts 1985, 69th Leg., R.S., ch. 409 \(H.B. 2375\), 1985 Tex. Gen. Laws 1499.](#)

⁶² *Id.*

1989

The 71st Legislature enacted the Information Resources Management Act, which abolished the AITC and established the Texas Department of Information Resources (DIR).⁶³ DIR was tasked with coordinating, directing, and planning for the use of information resources technologies by state agencies in addition to approving and improving information system procurements.⁶⁴ The Information Resources Management Act's passage marked the culmination of nearly four decades of legislative efforts to manage data processing, information resources, and technology in state government. Within DIR, an entity created solely for the purpose of addressing information resources and technology, the Information Resources Management Act consolidated many oversight roles that were decentralized across several agencies or addressed by individual state agencies with varying levels of experience and knowledge in the field.

For the first time, statute also conceptualized a comprehensive information resources management cycle.⁶⁵ This cycle included components related to strategic and operational planning, budgeting, procurement, and performance evaluation of information resources, projects managing these and other technology resources, and employees specifically within that field. Among its other roles, DIR was tasked with:

- Developing a state strategic plan every two years for information resources management;
- Compiling an annual statewide performance report on the state's use of technology;
- Monitoring national and international technology standards;
- Developing, publishing, and ensuring compliance with policies, procedures, and standards related to information resources management by state agencies; and
- Establishing an information resources technology evaluation center for use by DIR and other state agencies.

1991

The 72nd Legislature created the Telecommunications Planning Group, composed of DIR, the Comptroller of Public Accounts, and the General Services Commission, to develop a statewide telecommunications strategic operating plan for all state agencies.⁶⁶

1993

In 1993, DIR began its journey towards establishing a statewide technology center, analyzing state agency major information resources projects (MIRPs), and transitioning to a biennial

⁶³ [Acts 1989, 71st Leg., R.S., ch. 788 \(H.B. 2736\), 1989 Tex. Gen. Laws 3569.](#)

⁶⁴ [Id.](#)

⁶⁵ [Id.](#)

⁶⁶ [General Appropriations Act, 72nd Leg., 1st C.S., ch. 19 \(H.B. 1\), art. I, § 3, 1991 Tex. Gen. Laws 365, 588 \(Statewide Telecommunications\).](#)

performance report.⁶⁷

The General Appropriations Act (GAA) tasked DIR and Angelo State University with entering into a partnership to establish a State Data Recovery Facility and Operational Data Center at Angelo State University's San Angelo campus.⁶⁸

Additionally, the Legislature passed legislation repealing the requirement for DIR to review individual state agency technology procurements in addition to streamlining state agency reporting requirements to—amongst others—DIR.⁶⁹ This reporting enhancement—as well as DIR's growing presence in overseeing information resources and technology issues in state government—became more apparent as DIR was incorporated as a member of the GAA rider-created Quality Assurance Team (QAT).⁷⁰ The QAT is a collaborative group tasked with defining the quality assurance review process for MIRPs, specifically, the review and approval of these significant projects. In addition, the Legislature transitioned DIR's annual statewide performance report on the state's use of technology to a biennial report focused on reporting state agency progress on the goals identified by the state strategic plan.⁷¹

1995

The 74th Legislature clarified its legislative intent behind the West Texas Disaster Recovery and Data Operations Center, established through the partnership between DIR and Angelo State University pursuant to the 1994–1995 GAA rider, to indicate that “all state agencies and institutions of higher education utilize...the Center for testing disaster recovery plans and for disaster recovery services.”⁷² To further this legislative intent, the Legislature prohibited state agencies from using appropriated funds to enter into—or renew contracts for—testing disaster recovery plans and disaster recovery services.⁷³ Alternatively, state agencies could receive a waiver from DIR confirming that the services could not be provided through the Center. This rider ultimately set statutory direction for years to come regarding the consolidation of Texas' data. The Legislature directed DIR to collaborate with the Council on Competitive Governments (regarding issues concerning state data center consolidation) and report on the potential to use

⁶⁷ The 73rd Regular Legislature, through [Senate Bill 248](#), recodified statute and moved DIR's enabling legislation to Government Code Chapter 2054.

⁶⁸ [General Appropriations Act, 73rd Leg., R.S., ch. 1051 \(S.B. 5\), art. I, § 5, 1993 Tex. Gen. Laws 4518, 4704 \(State Disaster Recovery Facility and Operations Data Center\).](#)

⁶⁹ [Acts 1993, 73rd Leg., R.S., ch. 906 \(S.B. 381\), 1993 Tex. Gen. Laws 3811.](#)

⁷⁰ [General Appropriations Act, 73rd Leg., R.S., ch. 1051 \(S.B. 5\), art. 5, § 133, 1993 Tex. Gen. Laws 4518, 5387 \(Quality Assurance Review on Major Information Resources Projects\).](#)

⁷¹ [Acts 1993, 73rd Leg., R.S., ch. 906 \(S.B. 381\), § 13, 1993 Tex. Gen. Laws 3811, 3819.](#)

⁷² [General Appropriations Act, 74th Leg., R.S., ch. 1063 \(H.B. 1\), Article IX, § 40, 1995 Tex. Gen. Laws 5242, 6093.](#)

⁷³ *Id.*

the Center as a location for one of the state's consolidated data centers.⁷⁴

1996

The Sunset Advisory Commission issued its [staff report](#) on DIR, concluding that: DIR's functions were necessary to the state; DIR's activities to achieve its goals should be continued; and DIR's assigned duties that overlapped with similar responsibilities of other state agencies required specialized knowledge and expertise that positioned DIR as best situated to perform these duties. The Sunset Advisory Commission recommended the continuation of DIR for another 12 years. The Sunset Advisory Commission's other recommendations focused primarily on incremental changes to further improving DIR's interactions with the Legislature and other state agencies. These other recommendations included:

- Revising the statewide planning cycle for information resources management to better coincide with the state's strategic budgeting cycle;
 - Expanding DIR's role in providing quality assurance assistance to state agencies;
 - Better addressing rapidly changing state agency telecommunications needs by focusing the duties of the telecommunications planning group;
 - Enhancing the training and role of state agency Information Resources Managers; and
 - Revising the membership structure of the DIR Board of Directors to reflect recent legislative changes in DIR's mission.
-

1997

The 75th Legislature adopted legislation at the Sunset Advisory Commission's instruction continuing DIR for 12 years and further expanding DIR's authority over—and oversight of—MIRPs, state agency Information Resources Managers training (and their continuing education), and state agency biennial operating plans.⁷⁵ In addition to this expansion of DIR's previously existing responsibilities, the Legislature added internal quality assistance to DIR's duties and tasked DIR with the management of the Year 2000 Project Office, which included the creation and operation of the Year 2000 Project Office website and toll-free number.⁷⁶

The Legislature revised the DIR governing board's structure to allow for better customer (state agency) representation by adding statutorily identified ex officio members from state agencies.⁷⁷ To address DIR's growing role in the information resources and technology fields,

⁷⁴ *Id.*

⁷⁵ [Acts 1997, 75th Leg., R.S., ch. 606 \(S.B. 365\), 1997 Tex. Gen. Laws 2128.](#)

⁷⁶ [General Appropriations Act, 75th Leg., R.S., ch. 1452, art. IX, § 188, 1997 Tex. Gen. Laws 1452, 6430 \(Year 2000 Conversion\).](#)

⁷⁷ [Act 1997, 75th Leg., R.S., ch. 606 \(S.B. 365\), § 2, 1997 Tex. Gen. Laws 2128, 2129 \(codified as an amendment to Gov't Code § 2054.021\).](#)

the Legislature expanded potential conflicts of interest.⁷⁸ Furthermore, it separated the policymaking responsibilities of DIR's Board of Directors and the management responsibilities of DIR Executive Director and staff.⁷⁹ This separation preserved the DIR governing board's focus on the agency's policy and impact on state government information resources and technology.

1999

DIR's role as the knowledge leader in the electronic government field began in 1999; the Legislature ordered DIR to create a task force to assess the feasibility of establishing a common electronic system through which state agencies and constituents could conduct electronic transactions using the internet.⁸⁰ The task force constituted several state agencies, local governments, regulated businesses, and public members. DIR and this group, colloquially identified as the Electronic Government Task Force, developed a demonstration project, and reported on the project's success to the Legislature, which ultimately resulted in the TexasOnline program.

The Legislature also continued its GAA endorsement of DIR contracting with the Legislative Budget Board to execute quality assurance and oversight activities.⁸¹

2000

DIR restructured the Information and Communications Technology Contracts program to allow customers to order products and services directly from the vendor rather than through DIR.

In addition, DIR hosted its first Information Security Forum (ISF).

2001

The 77th Legislature authorized DIR's most significant growth yet with comprehensive legislation transforming the Texas information resources technology landscape. The most recognizable of these transformations was the creation of the DIR-managed TexasOnline, a project establishing the common electronic infrastructure through which state agencies and local government entities could electronically send and receive payments and documents.⁸² State leadership saw this program as an opportunity to provide a single point of contact for anyone—anywhere and at any time—to access e-government services available in Texas. As the leader of the TexasOnline Project, DIR became responsible not only for the implementation of

⁷⁸ [*Id.* at § 3, 1997 Tex. Gen. Laws 2128, 2129 \(codified at Gov't Code § 2054.022\).](#)

⁷⁹ [*Id.* at § 5, 1997 Tex. Gen. Laws 2128, 2130 \(codified at Gov't Code § 2054.029\).](#)

⁸⁰ [Acts 1999, 76th Leg., R.S., ch. 630 \(S.B. 974\), § 1, 1999 Tex. Gen. Laws 3189 \(codified at Gov't Code § 2054.062\).](#)

⁸¹ [General Appropriations Act, 76th Leg., R.S., ch. 1589 \(H.B. 1\), art. IX, § 9-6.22, 5446, 6285 \(Quality Assurance Review of Major Information Resources Projects\).](#)

⁸² [Acts 2001, 77th Leg., R.S., ch. 342 \(S.B. 187\), § 3, 2001 Tex. Gen. Laws 623 \(codified at Gov't Code Chapter 2054, Subchapter I\).](#)

Texas' electronic government, but also as a collaborator for all state agencies and other government entities interested in using TexasOnline.

Also in 2001, the Legislature abolished the General Services Commission, transferring its Telecommunications Division to DIR and creating the Telecommunications Planning and Oversight Council to oversee the planning and reporting functions of the division.⁸³

The Legislature completed streamlining Texas' state government technological landscape by statutorily designating DIR's Executive Director as the state's Chief Information Officer with authority for all aspects of information technology for state agencies.⁸⁴

2003

Two years after the creation of TexasOnline, the 78th Legislature amended statute with the express intention to allow greater access to the portal's services by:

- Allowing state agencies to use e-Pay, an online payment processing system, for over-the-counter transactions;
- Requiring state agencies to include a link to TexasOnline from their websites;
- Requiring additional state agencies to use the Common Occupational Licensing project; and
- Requiring DIR to create a web portal for veterans.⁸⁵

DIR's scope of strategic authority over information resources and technology grew during the 78th Legislative Session. The Legislature passed a bill that granted DIR additional review responsibilities over agency strategic plans and oversight of electronic government projects involving multiple state agencies designed to establish common information resources infrastructure.⁸⁶ DIR was also tasked with creating an information technology consolidation plan for state government.⁸⁷

Given the newness of technology, the Legislature continued to highlight DIR's collaboration with other entities through the creation of the Information Technology Council for Higher Education, which is a council composed of the Chief Information Officers of six of the largest

⁸³ [Acts 2001, 77th Leg., R.S., ch. 1422 \(S.B. 311\), 2001 Tex. Gen. Laws 5021.](#)

⁸⁴ [Acts 2001, 77th Leg., R.S., ch. 1272 \(S.B. 1458\), § 4.01, 2001 Tex. Gen. Laws 3049, 3057 \(codified at Gov't Code § 2054.0285\).](#)

⁸⁵ [Acts 2003, 78th Leg., R.S., ch. 1216 \(S.B. 1152\), 2003 Tex. Gen. Laws 3449 \(codified at relevant sections of Gov't Code Chapter 2054\).](#)

⁸⁶ This is the definition for consortia project, a term introduced by [SB 1701 \(78th RS\)](#) that is no longer used by statute.

⁸⁷ [Acts 2003, 78th Leg., R.S., ch. 1246 \(S.B. 1701\), § 3, 2003 Tex. Gen. Laws 3513 \(codified at Gov't Code § 2054.092\).](#)

public institutions of higher education systems, excluding public junior colleges.⁸⁸

Finally, after several years of riders authorizing the formation of the QAT, DIR received statutory acknowledgment for the QAT's creation and its MIRP review.⁸⁹ As of 2003, DIR, the Legislative Budget Board, and the State Auditor's Office collaboratively perform QAT-related tasks as detailed by statute and administrative rule.

2004

To better align with the state's expanding technology needs, DIR underwent an internal restructuring. This restructuring addressed DIR's growing breadth of responsibilities and demands placed upon the agency. Within this new structure, DIR evolved and was better able to rapidly respond to new opportunities, resulting in a more performance- and customer-driven agency.

DIR published its Biennial Performance Report, in which DIR emphasized the importance of reducing government costs, supported effective technology procurement and contracting, consolidated technology operations for increased efficiencies, and promoted the innovative use of technology that adds value to government services.

DIR established the state's first Chief Information Security Office after long observation and familiarity with best practices regarding the information resources and technology trends, including growing security risks.

DIR also published A Foundation for Change, which presented a roadmap for a shared IT infrastructure to support the missions of government agencies.

2005

Following DIR's publication of its 2004 Biennial Performance Report, the 79th Legislature enacted House Bills 1516 and 3112, which implemented many of the report's technology recommendations.⁹⁰ Furthermore, the passage of these bills signaled a larger adoption of a statewide shared IT infrastructure, first conceptualized back in 1993 with the incorporation of the GAA rider that instructed DIR and Angelo State University to collaborate on the creation of the State Data Recovery Facility and Operational Data Center.

This statewide enterprise approach to information resource and technology management and security ensured the security and maturity of state information resources and technology by:

⁸⁸ [Acts 2003, 78th Leg., R.S., ch. 1266 \(S.B. 1652\), § 3.02, 2003 Tex. Gen. Laws 3575, 3585 \(codified as an amendment to Gov't Code § 2054.121\).](#)

⁸⁹ [Acts 2003, 78th Leg., R.S., ch. 1246 \(S.B. 1701\), 2003 Tex. Gen. Laws 3513 \(codified as amendment to relevant sections of Gov't Code Chapter 2054\).](#)

⁹⁰ [Acts 2005, 79th Leg., R.S., ch. 1068 \(H.B. 1516\), 2005 Tex. Gen. Laws 3544; Acts 2005, 79th Leg., R.S., ch. 760 \(H.B. 3112\), 2005 Tex. Gen. Laws 2602.](#)

- Requiring state agencies to use DIR's contracts to purchase information resources and information resources technology commodities, and use the state data center if DIR determined that such use was cost-effective;
- Creating the Texas Project Delivery Framework, a method for the selection, control, and evaluation of information resources and information resource technologies for state agency use;
- Requiring DIR to provide network security services to certain state agencies and be responsible for network security from external threats to entities who use these services;
- Establishing and requiring DIR's management of the Network Security Center to provide network security system services for all state agencies using the Network Security Center; and
- Completing a biennial report on DIR's accomplishment of its network security service objectives and performance measures, and the status of the consolidated network security system provided through the Network Security Center.

During this time, DIR published its State Strategic Plan for Information Resources Management, which identified a plan for changing technology investment and management practices to ensure that Texas' business needs drove the state's technology.

2006

DIR prioritized 28 state agencies for inclusion in Data Center Services (DCS). In collaboration with these agencies, DIR developed the DCS request for offers, conducted the procurement, and awarded the contract. As part of its telecommunications duties, DIR amended the contract with its Texas Agency Network (TEX-AN) provider, resulting in significant technology enhancements, reduced costs for its diverse customer base, and a shared, statewide internet protocol communications platform for TEX-AN. In addition, five years after the state began the implementation of TexasOnline, the portal achieved financial "breakeven" for designated projects.

2007

DIR contracted with International Businesses Machines (IBM) for DCS in March 2007, to provide server services, mainframe services, and bulk print mail services, and to consolidate the infrastructure and its associated managed services. At the start of the contract, participating agencies began receiving services. As part of this effort, equipment for agency data was migrated to two locations: one in Austin (the Austin Data Center) and one at Angelo State University (the Center initially created through the 1993 GAA rider). The Austin Data Center became operational in June; in November, the Health and Human Services Commission became the first agency to move its print and mail operations to the data center.

The 80th Legislature transferred authority for an enterprise resource planning system from DIR

to the Comptroller of Public Accounts.⁹¹

DIR published the State Enterprise Security Plan for Fiscal Years 2007-2012, which provided goals, objectives, and a plan of action to safeguard the information resources of the state as consistent with the Texas Homeland Security Strategic Plan.

State agencies submitted their first Information Resources Deployment Reviews to DIR.

2008

DIR established a Performance Analytics Office to provide business intelligence, specifically customer spending and other trends, to the Information and Communications Technology Contracts program. At the Austin Data Center, the Texas Department of Agriculture, Texas Department of Transportation, Texas Workforce Commission, and the Office of the Attorney General all consolidated print and mail operations, and the Texas Youth Commission and Texas Workforce Commission completed their mainframe consolidations. Additionally, DIR completed the transformation of its own applications and application servers, all at the new Austin Data Center.

DIR opened the Network Security Operations Center (NSOC) to provide information security services to state agencies, including security event alerting and reporting, event correlation, and non-intrusive vulnerability scans.⁹²

2009

As cybersecurity and information technology became inextricably linked, the 81st Legislature strengthened DIR's cybersecurity program by granting DIR specific authority to develop rules regarding vulnerability testing of network hardware and software.⁹³ Furthermore, the Legislature signaled its faith in DIR's management of the telecommunications strategy and services for the state by eliminating the Telecommunications Planning and Oversight Council.⁹⁴

DIR's work on major IT goals and strategy for the state progressed, such as its efforts on TexasOnline and the consolidation of state agency information resources and technology in the Austin Data Center. DIR rebranded the TexasOnline portal as Texas.gov and entered into a new contract for the management of Texas.gov, effective January 2010.

The Texas Higher Education Coordinating Board, Texas Education Agency, Texas Department of Insurance, and Texas Department of State Health Services completed print and mail consolidation in the Austin Data Center while the Office of the Attorney General and the

⁹¹ [Acts 2007, 80th Leg., R.S., ch. 1089 \(H.B. 3106\), 2007 Tex. Gen. Laws 3714.](#)

⁹² [Gov't Code Chapter 2059, Subchapter C.](#)

⁹³ [Acts 2009, 81st Leg., R.S., ch. 183 \(H.B. 1830\), § 7, 2009 Tex. Gen. Laws 528, 531 \(codified at Gov't Code § 2054.060\).](#)

⁹⁴ [Acts 2009, 81st Leg., R.S., ch. 393 \(H.B. 1705\), 2009 Tex. Gen. Laws 970.](#)

Railroad Commission of Texas completed their mainframe consolidation in the Austin Data Center.

2010

The newly rebranded Texas.gov received several awards and recognitions for its performance.

As DIR transitioned DCS to an owner-operator governance model to involve customer agencies in the decision-making process, the re-procurement of DCS services moved forward with DIR's release of two Data Center Services Requests for Offers.

Additionally, DIR began the substantial lift to innovate and transform the telecommunications system in the Capitol Complex from the 35-year-old Capitol Complex Telephone System (CCTS) private branch exchange (PBX) voicemail and phone system to a fully integrated Voice over Internet Protocol (VoIP) platform, a transition that marked a substantial advancement in modernizing the communications infrastructure and catering to the state of Texas' evolving needs.

2011

The Sunset Advisory Commission issued its final report on DIR, following the passage and subsequent gubernatorial veto of House Bill 2499 (DIR's sunset bill); this report encouraged the continuation of DIR, emphasizing that DIR provides critical services needed by all state agencies.⁹⁵ Even though the Sunset bill itself was vetoed following the 82nd Regular Session, the Legislature still adopted several of the Sunset Advisory Commission's recommendations and additional legislative provisions relating to the Sunset review of DIR in other legislation during the 82nd First Special Session.⁹⁶ These recommendations and provisions included:

- Continuing DIR until 2014 and directing the Sunset Advisory Commission to re-examine the agency and make recommendations to the 83rd Legislature;
- Transferring a portion of DIR's surplus fund balances to General Revenue, which resulted in a gain of \$4.3 million to the General Revenue fund;
- Increasing the monitoring and oversight of DIR's appropriations;
- Improving oversight of DIR's contracts and clarifying revolving door provisions; and
- Keeping the Cooperative Contracts program at DIR but requiring DIR to obtain services of the best value and consider using strategic sourcing.⁹⁷

In addition to the Sunset-related legislation described above, the Legislature amended statutory references from "TexasOnline" to the "state electronic Internet portal" to ensure the

⁹⁵ [Tex. H.B. 2499, 82nd Leg. R.S. \(2011\).](#)

⁹⁶ [Acts 2011, 82nd Leg., 1st C.S., ch. 4 \(S.B. 1\), art. 23, 2011 Tex. Gen. Laws 5254, 5280 \(codified at relevant sections of Gov't Code Chapter 2054\).](#)

⁹⁷ [Id.](#)

longevity of statutory references made to the official website for the State of Texas.⁹⁸

DIR completed the initial contract review and award for TEX-AN Next Generation services, which offered agencies and other eligible state customers a broader array of telecommunications services and vendor choices.

Additionally, DIR established its Internal Audit department to identify necessary or recommended improvements to DIR's programs including the facilitation and implementation of those changes.

2012

DIR reorganized the Information and Communications Technology Cooperative Contracting Division as the Technology Sourcing Office to better reflect the services and offerings that DIR was making available through its statutory authorization to source for commercially reasonable information technology commodities on behalf of the state.

DIR awarded three contracts for DCS-related services:

- Multi-sourcing Services Integrator (MSI) to Capgemini;
- Server and Mainframe Services to ACS, Inc.; and
- Bulk print mail to Xerox.

DIR began migration efforts to the shared VoIP platform, upgrading systems as necessary to effectively support multiple agencies.

2013

The Sunset Advisory Commission completed its [final report](#), conducted in compliance with the 82nd Legislature's mandate for the Sunset Advisory Commission to re-examine DIR. In this report, the Sunset Advisory Commission made recommendations to the 83rd Legislature. The 82nd Legislature's passage of Sunset-related bills addressed various needs associated with DIR and significantly altered DIR's way of doing business, which resulted in a broader final report that took a wait-and-see approach, continuing DIR for another eight years to allow for greater collection of data related to the changes that the Legislature authorized two years prior.

The 83rd Legislature passed a Sunset bill that incorporated several Sunset Advisory Commission recommendations from the 2011 final report making statutory revisions necessary to ensure the ongoing implementation of changes made to DIR's oversight, management of administrative fees and costs, and contracting practices since 2011.⁹⁹ These changes included:

⁹⁸ [Acts 2011, 82nd Leg., R.S., ch. 973 \(H.B. 1504\), 2011 Tex. Gen. Laws 2427 \(codified at relevant sections of statute\).](#)

⁹⁹ [Acts 2013, 83rd Leg., R.S., ch. 48 \(H.B. 2472\), 2013 Gen. Tex. Laws 98.](#)

- Creating the Customer Advisory Committee to report to and advise the DIR Board of Directors on DIR's delivery status of critical statewide services;
- Requiring the DIR Board of Directors to appoint a neutral Internal Auditor who reports directly to the DIR Board of Directors and provide appropriate resources to support that position's work, including the completion of an annual audit plan for DIR;
- Creating a DIR Board of Directors audit subcommittee that provides oversight of the appointed auditor, other audit issues, and whether the Internal Auditor has sufficient resources;
- Enhancing DIR Board of Directors oversight of DIR strategic services, fulfillment of its mission, and evaluation of its department operations;
- Mandating that DIR adopts a process and clear procedures to determine its programmatic administrative fees and ensure that such fees are directly related to recouping the cost of operations;
- Establishing an annual report submitted by DIR to the Legislative Budget Board of any administrative fees it sets (including the analysis and methodology used to determine the fee amounts and the cost allocation charged to customers) and post information about the administration fees;
- Instructing the Comptroller of Public Accounts to create in the state treasury a Statewide Technology Account, into which all money DIR received under Government Code Chapter 2055, Subchapter L, shall be deposited for the operation and management of a statewide technology center or for any other purpose specified by the Legislature; and
- Requiring the DIR Board of Directors to approve and oversee major outsourced contracts as defined by DIR rule and have DIR staff develop contract management plans for major outsourced contracts in consultation with the DIR Board of Directors.¹⁰⁰

In addition to these Sunset-related amendments, the Legislature determined that there was a lack of a coordinated cybersecurity effort across the state, which it addressed by passing significant legislation identifying DIR as the nexus for cybersecurity coordination in the state, expanding DIR's ability to address cybersecurity needs.¹⁰¹ The Legislature authorized DIR to use available funds to protect the cybersecurity of state agency information, establishing the position of the Cybersecurity Coordinator, a role designated by the DIR Executive Director to facilitate and cultivate partnerships between public and private entities that are necessary to

¹⁰⁰ *Id.*

¹⁰¹ [Acts 2013, 83rd Leg., R.S., ch. 32 \(S.B. 1102\), 2013 Tex. Gen. Laws 40](#); [Acts 2013, 83rd Leg., R.S., ch. 477 \(S.B. 1134\), 2013 Tex. Gen. Law 1325](#).

the collective cybersecurity of Texas.¹⁰² In addition to building these partnerships, the Cybersecurity Coordinator would be responsible for establishing and leading the Texas Cybersecurity Council.¹⁰³

Additionally, the 83rd Legislature directed DIR to perform a legacy systems study detailing the use of legacy systems and software state agencies, excluding institutions of higher education, to evaluate the composition of the state's current technology landscape and determine how best to approach and make decisions about aging infrastructure.¹⁰⁴

2013 marked the last substantial increase in DIR's full-time equivalent (FTE) employee count with DIR's headcount remaining relatively the same since that time until the 88th Legislature approved an additional 39 FTEs.

2014

Following the significant growth in its cybersecurity responsibilities and authorization to use available funds to ensure the cybersecurity of the state, DIR established the Texas Cybersecurity Framework (TCF), the InfoSec Academy, and the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) to assist agencies in reporting security incidents and their security maturity based on the TCF. Pursuant to its statutory requirements, DIR appointed its Chief Information Security Officer as the Cybersecurity Coordinator and established the Texas Cybersecurity Council.

DIR leveraged its administrative rules on information security to adopt security controls based on the National Institute of Standards and Technology's (NIST) Security and Privacy Controls for Information Systems and Organizations (800-53) that state agencies were required to use for their own information security needs.¹⁰⁵ Additionally, DIR began offering security assessments according to the TCF to give state agencies the ability to have an independent security assessment funded by DIR.

DIR published the first Biennial Information Security Report, reporting on the maturity levels of the state agencies and institutions of higher education according to the TCF.

DIR released the legislatively required Legacy Systems Study, in which it identified the current landscape of legacy systems across the state and the cost of maintaining these systems. In the Legacy Systems Study, DIR also made recommendations on how to address these issues, such as recommending that state agencies develop a prioritized impact analysis and mitigation plan

¹⁰² [Acts 2013, 83rd Leg., R.S., ch. 32 \(S.B. 1102\), § 1, 2013 Tex. Gen. Laws 40 \(codified at Gov't Code § 2054.551\).](#)

¹⁰³ *Id.*

¹⁰⁴ [Acts 2013, 83rd Leg., R.S., ch. 182 \(H.B. 2738\), § 1, 2013 Tex. Gen. Laws 829 \(codified at Gov't Code Chapter 2054, Subchapter O\).](#)

¹⁰⁵ 1 Tex. Admin. Code §§ [202.24](#), [202.74](#).

of identified legacy system security risks.

2015

Following DIR's publication of the Legacy Systems Study, the 84th Legislature passed legislation¹⁰⁶ enacting many of the recommendations made by the study, including:

- Requiring DIR to collaborate with other state agencies, not including institutions of higher education, to develop a legacy system modernization strategy to guide the state in its legacy system modernization efforts;
- Implementing a shared data reporting and business analytics service, and a shared Application Portfolio Management (APM) program for use by state agencies; and
- Identifying information security issues associated with legacy systems and developing a plan to prioritize the remediation and mitigation of those issues.

In addition to the traction on information security for legacy systems, DIR endeavored to ensure the effectiveness and security of the state telecommunications network by continuing its work on migrating all state agencies in the Capitol Complex Telephone System to VoIP platform, all while upgrading the VoIP platform to a Hosted Collaboration Solution (HCS) multi-tenant platform. The switch to an HCS multi-tenant platform made it possible to concurrently service and support multiple agencies and allow each agency to have its own isolated and secure environment. DIR assumes responsibility for platform maintenance, upgrades, and ongoing support while state agencies receive customized services based on individual requirements.

DIR expanded the Information Security Forum (ISF) and began holding the event at the Palmer Events Center to accommodate growing attendance, which included local government entities beginning in 2015.

The 84th Legislature addressed the need to improve data governance and the coordination of interagency data collection and data by creating the role of the statewide Data Coordinator at DIR to oversee statewide data issues.¹⁰⁷

2016

The DCS program met its consolidation goals with mainframe, print and mail, server, and service desk services fully consolidated.

Internally, DIR reorganized the Technology Sourcing Office and rebranded it as the Chief Procurement Office.

¹⁰⁶ [Acts 2015, 84th Leg., R.S., ch. 460 \(H.B. 1890\), 2015 Tex. Gen. Laws 1774.](#)

¹⁰⁷ [Acts 2015, 84th Leg., R.S., ch. 1047 \(H.B. 1912\), 2015 Tex. Gen. Laws 3663.](#)

2017

DIR continued to expand the offerings available to eligible customers through the Shared Technology Services (STS) program when it awarded two Managed Application Services contracts, adding managed application services for application development and maintenance, and for application services-rate card. These contracts allowed customers to reinvest infrastructure consolidation savings to continue modernizing legacy applications. In addition to these additions, DIR began expanding its STS offerings to include hybrid public cloud capabilities.

The 85th Legislature further signaled its faith in DIR to lead the cybersecurity efforts of the state by passing legislation that led to increased cybersecurity responsibilities for DIR.¹⁰⁸ These responsibilities included assisting the Sunset Advisory Commission in assessing the cybersecurity practices of agencies the Commission reviews and establishing a statewide incident response working group. This legislation required DIR to lead a collaborative group composed of DIR, the Texas Military Department, Texas Department of Public Safety, and the Texas Division of Emergency Management to develop a plan to address cybersecurity risks and incidents in this state. This collaboration became known as the Statewide Incident Response Workgroup; the workgroup documented how the state would address overwhelmed local response capability in the scenario of a large-scale or statewide cybersecurity incident while building relationships between the workgroup collaborators, state leadership, state agencies, and local governments.

The first iteration of Texas.gov was a public-private partnership (P3) model, wherein Texas established a contractual partnership with a private entity to finance the TexasOnline project up front. The proceeds from the project then went to the financing party. After almost a decade of success with Texas.gov, however, the 85th Legislature authorized Texas.gov funding to flow through DIR to an established certified public accountant (CPA) rather than through a private-sector third party.¹⁰⁹ This switch effectively eliminated the P3 model in place and allowed the program to move to a traditional cost-of-services model similar to the DCS program.

Following the passage of this legislative authorization, DIR opened its re-procurement of Texas.gov at the end of August. The procurement included two significant changes from previous iterations of Texas.gov:

- Eliminating the P3 model previously established; and
- Separating the duties between application development services and payment processing services.

¹⁰⁸ [Texas Cybersecurity Act, 85th Leg., R.S. ch. 683 \(H.B. 8\), §§ 11, 15, 2015 Tex. Gen. Laws 3027 \(codified at relevant sections of Gov't Code Chapter 2054\).](#)

¹⁰⁹ [General Appropriations Act, 88th Leg., R.S., ch. 605 \(S.B. 1\), art. I, § 8, 2017 Tex. Gen. Laws 1648, 1729 \(Texas.gov Project and the Statewide Network Applications Account\).](#)

DIR also began supporting efforts to grow the cybersecurity workforce of tomorrow by contributing to GirlsGoCyberstart, a nationwide contest to get more high school girls interested in cybersecurity. Texas teams that finished highest in the competition came to Austin to meet the Governor and their district's state representative.

2018

DIR rebranded DCS as STS to reflect an expansion in services based on customer demands. DIR awarded two contracts under the Texas.gov procurement. Under these contracts, two separate vendors would provide the services necessary to support Texas.gov with Deloitte Consulting providing Texas.gov application development services and Texas NIC providing Texas.gov payment processing. Due to the growth and critical nature of the Texas.gov program, DIR added it to DIR's outsourced managed services provided through the DCS program. Additionally, DIR executed a digital Multi-Sourcing Services Integrator (MSI) that further enhanced the abilities of the program.

Within the newly rebranded STS, DIR established the Managed Security Services (MSS) program, which provided various security services to customers eligible for Shared Technology Services. Through the MSS program, DIR was able to provide penetration tests and Texas Cybersecurity Framework (TCF) assessments for state agencies and institutions of higher education. The MSS program further ensures the security of the state's data and networks by making available to eligible customers other types of assessments, penetration tests, incident response services, security monitoring services, and device management services. The Cybersecurity Operations team utilizes security operations center services through MSS.

After a year of DIR's Chief Information Security Officer concurrently serving as the Cybersecurity Coordinator, DIR determined that the role demanded a full-time employee dedicated strictly to the enumerated statutory responsibilities, placing a job posting for a full-time Cybersecurity Coordinator in 2018. DIR applied to the State Homeland Security Grant Program to aid in funding the Cybersecurity Coordinator role.

In response to various legislative requirements passed during the 85th Legislative Session, DIR acted on several documents including:

- Drafting and publishing the [Information Resources Employees Continuing Education Guidelines for Cybersecurity](#);
- Updating the security plan process developed in 2014 to include a biennial Data Security Plan for Online and Mobile Applications for impacted agencies; and
- Publishing the first Biennial Cybersecurity Report.

2019

The 86th Legislature increased DIR's responsibility relating to the cybersecurity of information resources following the Senate Select Committee on Cybersecurity's identification of areas that could benefit from improvement. Cybersecurity legislation passed during the session intended to address these issues by improving Texas' cybersecurity to protect data and ensure that key services are delivered. These initiatives would strengthen the state's oversight of cybersecurity

by bolstering the cybersecurity workforce, assisting local government entities recovering from cybersecurity incidents, and improving oversight of the electric grid. The Legislature assigned most of these tasks to DIR due to its unique role at the nexus of addressing cybersecurity and information resources needs for the state.¹¹⁰ These identified duties and tasks included:

- Certifying at least five cybersecurity training programs for use by government entities required to complete annual certified training;
- Collaborating with the Texas Higher Education Coordinating Board to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity, and consult with the Texas Higher Education Coordinating Board to coordinate with lower-division institutions of higher education and post-secondary certification programs to develop cybersecurity certification programs;
- Extending requirements to comply with DIR-established cybersecurity and information security initiatives to entities not previously subject to those requirements;
- Establishing an information sharing and analysis organization that provides a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats and best practices;
- Drafting the Prioritized Cybersecurity and Legacy Systems Report, a biennial report intended to allow DIR to recommend prioritization of funding for state agency cybersecurity projects and state agency projects to modernize or replace legacy systems; and
- Requiring the DIR-designated Cybersecurity Coordinator to collaborate with the Texas Cybersecurity Council and public and private entities in the state to develop best practices for cybersecurity and establish a Cyberstar Certificate program that recognizes entities that comply with these best practices.

In addition to the cybersecurity duties described above, the 86th Legislature appropriated funds to DIR to provide multi-factor authentication (MFA) to state agencies and institutions of higher education.¹¹¹ In response to the legislative actions of the 86th Session, DIR established an MFA program with staff to support it, a program to certify cybersecurity training programs, and a process to collect state and local government organizations' compliance with cybersecurity training requirements.

¹¹⁰ [Acts 2019, 86th Leg., R.S., ch. 1308 \(H.B. 3834\), 2019 Tex. Gen. Law 3856; Acts 2019, 86th Leg., R.S., ch. 509 \(S.B. 64\), 2019 Tex. Gen. Law 1359; Acts 2019, 86th Leg., R.S., ch. 573 \(S.B. 241\), 2019 Tex. Gen. Laws 1595.](#)

¹¹¹ [Supplemental Appropriations Act, 87th Leg., R.S., ch. 7 \(H.B. 5\), § 12 \(Department of Information Resources: Cybersecurity\).](#)

The 86th Legislature amended statutes related to the statewide Data Coordinator position to establish the state's first Chief Data Officer.¹¹² Following the passage of this bill, DIR appointed the state's first Chief Data Officer.

To further support its cybersecurity responsibilities and defray state costs, DIR applied for and received State Homeland Security Grant Program funding to hire program support staff to assist the Cybersecurity Coordinator in the execution of their statutory duties.

The Statewide Incident Response Workgroup's efforts to document the statewide strategic response to a cybersecurity incident proved crucial to government entities' recovery from a ransomware attack. In the early morning hours of August 16, 2019, [23 local governments found themselves impacted by the same ransomware attack](#), marking the first time that the Governor issued a disaster declaration for a cybersecurity incident. Through the dedication and vision of DIR's Office of the Chief Information Security Officer in the years prior to this attack, the state of Texas had a comprehensive and practiced response plan already in place and ready to be put into immediate action. Within hours of receiving notice of the event, DIR mobilized state and federal teams to the field at the most critically impacted sites to begin eradicating the malware and assessing impacts to systems. After less than a week, all impacted entities were cleared for remediation and recovery. DIR not only led the execution of the plan, but it also worked closely with the federal and state investigations into the attack which resulted in the arrest and extradition of the cybercriminal responsible for this attack and many others.

Within STS, DIR launched Texas by Texas (TxT), with the Texas Department of Licensing and Regulation as the first agency to make use of TxT to process massage therapist license renewals. DIR also began its solicitation of the Next Generation DCS for:

- Texas private cloud, facilities, and computing services;
- Technology solution services;
- Print, mail, and digitization services;
- Security operations services;
- Public cloud manager services; and
- Mainframe services.

2020

On March 13, 2020, the Office of the Governor issued a disaster declaration in response to the COVID-19 pandemic. This declaration resulted in an unprecedented demand for information resources and technology, both to allow state agencies to address a newly remote workforce and to support the demands upon agency technological resources by Texans requiring support.

Operationally, DIR doubled the state's redundant internet capacity from 10GB to 20GB within two weeks of the issuance of the disaster declaration. DIR assisted over 50 state agencies that submitted approximately 4,000 COVID-19 service requests to enable work from home

¹¹² [Act 2019, 86th Leg., R.S., ch. 604 \(S.B. 819\), 2019 Tex. Gen. Laws 1772.](#)

capabilities and increased the Capitol Complex Telephone System (CCTS) trunk lines by almost 100 percent to facilitate increased work from home demand on the Capitol Complex.

In addition to state agency demands to support their remote workforce, DIR provided resources expanding the state's ability to respond to the workforce crisis as individuals found themselves unemployed. DIR increased mainframe and service platforms for the Texas Workforce Commission and assisted in the migration of its main website to a government cloud to aid in stabilizing the unemployment website due to unprecedented high demand. DIR prioritized the Texas Workforce Commission's print and mail demands to allow for continued service to the growing number of Texas' unemployed population.

As part of its response to the pandemic, DIR created a webpage where it posted town halls and published numerous resources. These presentations and documents included best practices, guidance, and recommendations on:

- Cyber hygiene;
- Using cooperatives contracts for remote access and remote learning tools, products, and services;
- Remote work;
- Virtual private network (VPN) accessibility;
- Using the Open Data Portal to address public information requests;
- Managing technology risk during COVID-19; and
- Revising teleconferencing standards for a government body's open meetings.

DIR shared these resources across DIR's social media platforms, including LinkedIn, Twitter, and YouTube. In addition, DIR established recurring segments, called the "Cyber Corner," on Texas.gov to share useful cybersecurity information with the public. Although DIR found itself at the forefront of the state's response to the pandemic, DIR's execution of the other areas of its mission were not compromised.

In the field of cybersecurity, DIR's leadership of the statewide response to the August 2019 ransomware event was so successful that the federal Senate Committee for Homeland Security and Governmental Affairs invited DIR's Executive Director to testify in February 2020. The purpose of this testimony was for the federal government to learn more about Texas' successful state cyber response and how this success might be replicated across the country.

By the end of the fiscal year DIR certified its first set of cybersecurity training programs for use by state and local governments.

DIR's work on STS evolved as a best-in-breed service delivery model with the award of multiple contracts supporting the Next Generation DCS model. This approach uses multiple cross-functional contracts to develop and maintain statewide technology centers, information resources, and software applications. DIR awarded the following contracts to support this effort.

- **Texas Private Cloud, Facilities, and Computing Services to Atos IT Solutions and Services, Inc (Atos).** Under this contract, Atos provides server computing, data center facilities, and network management services for DIR's government customers.

- **Technology Solution Services (TSS) to Deloitte Consulting LLP (Deloitte).** Technology Solution Services (TSS) to Deloitte Consulting LLP (Deloitte). Deloitte provides DIR's government customers with technical strategy management, solution design, and project delivery for DCS public and private cloud infrastructure. This contract also provides for managed application services to include application development, maintenance, and staff augmentation services for applications hosted in the DCS program's public and private clouds. DIR developed the solicitation documents for the TSS procurement based off both market research and input from DIR's customer agencies who expressed a strong need for solutioning services that could, among other things, be rapidly deployed for small projects or in times of emergency. TSS served precisely this purpose for the Department of State Health Services during the COVID-19 pandemic. TSS completed 15 projects modernizing five DSHS applications improving DSHS response and utilization of data and ability to efficiently inform state leadership during the COVID-19 outbreak. Using TSS to complete these upgrades, DSHS avoided using emergency procurements when upgrading and modernizing their applications, and these projects met targeted budget and completion timelines.
- **Security Operations Service to Science Application International Corporation (SAIC).** SAIC provides cybersecurity policies, oversight, and monitoring of the DCS infrastructure.
- **Print, Mail, and Digitization Services to Xerox, Corp (Xerox).** Under this contract, Xerox manages large, recurring, and one-time print jobs of various sizes and complexities that are sorted, inserted, and mailed, leveraging volume postal discounts. This contract also allows for digitization of records for more efficient storage. Services are delivered from the state's Austin Data Center.
- **Public Cloud Manager to Rackspace US, Inc. (Rackspace).** Under this contract, Rackspace provides cloud computing operational support, technical and security assurances, and onboarding of public cloud services.
- **Mainframe Structure to Atos Government IT Outsourcing Services, LLC (Atos).** Under this contract, Atos provides mainframe computer, storage, database management, and production operations for DIR's STS customers.

In addition to the above-described contract awards, DIR released the Texas.gov Digital Identity Solution to certain state agencies. This solution provided enhanced MFA capabilities, ensuring the continued security of state information and networks.

DIR also received the Global Electronics Council 2020 Electronic Product Environmental Assessment Tool (EPEAT) Purchaser Award that is given to entities that demonstrate achievement in the procurement of sustainable IT products.

2021

The 87th Legislature passed a comprehensive bill aimed at strengthening the cybersecurity

posture, data security, and data management of the state.¹¹³ Among other requirements, Senate Bill 475 tasked DIR with creating a statewide Risk and Authorization Management Program, a Volunteer Incident Response Team, a Data Management Advisory Committee composed of designated agency Data Management Officers, and regional cybersecurity working groups. Additionally, DIR was charged with establishing a pilot Regional Security Operations Center (RSOC). Other legislation encouraged state agencies to use TxT instead of duplicating existing technology resulting in cost savings to the state and allowing the state to provide a secure, centralized, mobile-friendly portal to constituents.

In addition to SB 475, DIR received additional funding for the following initiatives:

- Data Optimization/Warehouse Project, which allows DIR to replace its legacy data warehouses to produce and provide efficient, reliable data analytics internally, for customers, and for state leadership.
- Endpoint detection and response (EDR) technology for state agencies, which allows DIR to purchase EDR technology and implement it at no cost to participating state agencies to better protect them from ransomware and other cyber threats.
- RSOC pilot, which allows DIR to partner with a public institution of higher education to establish the Security Operations Center pilot program authorized by SB 475.

In support of these legislative initiatives, DIR established the Texas Risk Authorization and Management Program (TX-RAMP) for cloud computing services, implementing administrative rules reflecting the requirements of the program and a program manual establishing the necessary procedures for TX-RAMP compliance. DIR modified its annual cybersecurity training program to allow for reporting by local governments and school districts and stood up a portal permitting state leadership to search for program compliance, so that grant applications could be reviewed for compliance with the cybersecurity training program requirements.

DIR formed both the Cybersecurity Incident Response Team (CIRT)¹¹⁴ and the statutorily created Volunteer Incident Response Team (VIRT).¹¹⁵ These teams safeguard the state's critical assets by sharing threat intelligence and offering incident response support to eligible organizations.

DIR began its process of implementing the RSOC by posting the [Regional Security Operations Center Expression of Interest Overview](#). The expression of interest invited all interested public institutions of higher education to submit proposals explaining why their institutions should be selected as the pilot RSOC under SB 475.

In addition to its newly created legislative duties, DIR announced the formation of the Texas

¹¹³ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\)\(codified at relevant sections of the Government Code\)](#).

¹¹⁴ [General Appropriations Act, 88th Leg., R.S., ch. 1053 \(S.B.1\), Art. IX, § 18.37 \(Contingency for Senate Bill 475\)](#).

¹¹⁵ [Gov't Code Chapter 2054, Subchapter N-2](#).

Artificial Intelligence Center of Excellence (AI-CoE) to accelerate innovation and safe adoption of artificial intelligence (AI) technologies. The AI-CoE leveraged the knowledge of DIR experts and key industry partners to develop AI skills in state agency information technology leaders and encourage collaboration and innovation to expedite solutions for the public sector. The AI-CoE focused on all branches of AI, including robotic process automation, machine learning, natural language processing, computer vision, and contact center technologies.

In February 2021, Winter Storm Uri descended upon Texas, resulting in severe winter weather that left many Texans without electricity. Prior to the storm's arrival, the Governor directed certain state agencies, including DIR, to report to the Statewide Operations Center to ensure that resources could be quickly mobilized to address Texans' needs. DIR worked closely with the Texas Facilities Commission to ensure that the generators at both the Sam Houston and Network Security Operations Center (NSOC) buildings were in good operational order and topped off with fuel, in addition to confirming that the Texas Facilities Commission had fuel on retainer and access to backup generators in case a generator failed at one of these vital facilities.

Winter Storm Uri caused network outages for telecommunications carriers across the state, which affected Atos' Data Center Network (DCN) ring, resulting in the failure of a portion of the DCN ring. To ensure the resiliency of Atos' network for their cloud and replicating services, DIR stepped in and provided an alternative network path that allowed DIR and Atos to collaboratively migrate the DCN traffic from Atos' DCN network to the DIR network. This joint effort allowed uninterrupted services for cloud and replicating offerings until the DCN network could be fully restored.

In August 2021, to ensure the efficiencies created by the data center services program continue in the face of changing technology, DIR obtained the approvals required by law and created the Application Services Center, a new statewide technology center to facilitate the expected shift toward cloud-driven software applications.

On November 8, 2021, the Federal Bureau of Investigation (FBI) announced its indictment of the individual suspected of the August 2019 ransomware attack against 23 government entities. DIR worked tirelessly with its federal partners during this investigation.

DIR launched a major redesign of the [Texas.gov website](https://www.texas.gov). The upgraded site improved the user experience with a new, mobile-friendly, ADA-accessible, and easy-to-navigate interface, enabling Texans to access the information or government services they need quickly and securely. This upgrade also provides secure, direct access to more than 800 official government services, including vehicle registration renewals, driver's license and ID renewals, vital records, professional and occupational licenses, and recreational and hunting licenses. DIR and the Texas Department of Public Safety announced the availability of driver's license renewals and vehicle registration renewals through TxT.

DIR and its staff were recognized for excellent work and innovation in the fields of information resources, cybersecurity, and technology throughout 2021:

- DIR was named a Top Workplace in the Greater Austin Area by the Austin American-Statesman.
- DIR won the Global Electronics Council 2021 EPEAT Purchaser Award.
- DIR Artificial Intelligence Center of Excellence (AI-CoE) received the StateScoop State IT Innovation of the Year Award.
- DIR's Chief Technology Officer and Deputy State Chief Information Officer John Hoffman was recognized by the National Association of State Technology Directors with an Honorary Life Membership.
- DIR's Chief Information Security Officer Nancy Rainosek received the 2021 Thomas M. Jarrett State Cybersecurity Leadership Award from the National Association of State Chief Information Officials (NASCIO). This award honors state CISOs for exceptional accomplishments in their field.
- DIR's Chief Operations Officer Dale Richardson received one of three 2021 National Association of State Chief Information Officials (NASCIO) State Technology Innovator Awards, which recognize outstanding state government employees who contributed to advancing state technology policy through the promotion of best practices, adoption of new technologies, and advancements in service delivery.
- DIR's Statewide Incident Response Coordinator Jonathan King received the Rising Star Award from the Texas Association of State Systems for Computing and Communications.

2022

DIR officially launched TxT, a digital assistant that allowed Texans to create an online account, manage their government-issued licenses and registrations, receive proactive reminders when it's time to take action, and complete transactions quickly and securely. The release of this digital assistant marked the culmination of years of effort aimed at aligning the way Texans consume government services with the streamlined, one-stop-shop experience they expect in other aspects of their lives. Just six months after launching, more than 1.6 million Texans created their accounts, effectively serving over 10 percent of the state's eligible population.

DIR's implementation of cybersecurity legislation continued into 2022. With the Texas Risk and Authorization Management Program (TX-RAMP) fully implemented, DIR began certifying cloud computing services in alignment with the process established by the TX-RAMP program manual.

DIR addressed other statutory initiatives when it launched the Texas Cyberstar Certificate program, a voluntary certificate recognizing public and private organizations that meet established criteria for cybersecurity best practices, and the Texas Information Sharing and Analysis Organization (TX-ISAO) portal to provide an efficient and secure method to share indicators of compromise (IOCs) and other actionable intelligence and events with the public and private sector members of the ISAO.

DIR made headway on its requirement to establish a RSOC when it selected Angelo State

University to host the pilot RSOC; DIR and Angelo State University then immediately began their collaboration to establish and implement the RSOC.

In September 2022, DIR's Chief Information Security Officer, Nancy Rainosek, was appointed to the Multi-State Information Sharing and Analysis Center (MS-ISAC) executive committee. The MS-ISAC is a division of the Center for Internet Security funded by the federal Cybersecurity and Infrastructure Security Agency (CISA) and provides cyber threat prevention, protection, response, and recovery resources for more than 13,000 U.S. state, local, tribal, and territorial (SLTT) government organizations that are members. This appointment marked unique federal recognition of DIR and its Chief Information Security Officer's role as a leader in state and national cybersecurity.

In December 2022, the Office of the Governor issued a letter to the heads of state agencies and institutions of higher education instructing them to ban the use of TikTok; this letter instructed DIR and the Texas Department of Public Safety to collaborate on a model policy for other state agencies to emulate.

DIR and its staff were recognized for excellent work and innovation in the fields of information resources, cybersecurity, and technology throughout 2022:

- DIR was named a Top Workplace in the Greater Austin Area by the Austin American-Statesman for the second consecutive year in a row.
- DIR was named a Top Workplace in the U.S. among employers with 150-499 employees.
- DIR won the Global Electronics Council 2022 EPEAT Purchaser Award.
- Texas by Texas was awarded State IT Innovation of the Year by StateScoop.
- Texas by Texas won the National Association of State Chief Information Officials (NASCIO) 2022 State IT Recognition award for Digital Services: Government to Citizen.
- DIR's Executive Director and Texas Chief Information Officer, Amanda Crawford, was recognized as the Golden Gov - State Executive of the Year by StateScoop.
- DIR's Chief Experience Officer (at the time known as the Director of Program Development), Endi Silva, received the Rising Star award from the State Agency Council to the Governor's Commission for Women.
- DIR's Chief Data Officer, Ed Kelly (now retired), was named one of the 100 most influential people in data in 2022 by the website DatalQ.
- DIR was recognized by WeHireVets for having a workforce that is composed of more than 10 percent veterans.

2023

In compliance with the [Governor's December 2022 directive](#), DIR collaborated with the Texas Department of Public Safety to create and publish a model policy banning the use of TikTok and other prohibited technologies on devices used for state businesses. The Governor's directive required all organizations to submit their policies to DIR with approval of the policies

to come from the Texas Department of Public Safety. DIR implemented a submission functionality for these policies through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) in mid-January.

The 88th Legislative Session continued the expansion of DIR's cybersecurity responsibilities, given its ongoing innovation in the fields of cybersecurity, information resources and technology, and data management. The Legislature passed bills requiring local governments to comply with DIR rules regarding security reporting,¹¹⁶ establishing the statewide Chief Information Security Officer role within DIR,¹¹⁷ and prohibiting the use of certain social media applications and services on devices owned or leased by government entities.¹¹⁸

In addition to these cybersecurity responsibilities, the Legislature tasked DIR with determining whether developing a state information technology credential to be offered by public junior colleges was a viable option to address shortages in the state information resources workforce;¹¹⁹ the Legislature provided DIR an avenue by which DIR could, at its discretion, collaborate with a public junior college to provide such a credential.¹²⁰

DIR also received additional appropriated funding from the Legislature to:

- Establish two additional Regional Security Operations Centers (RSOCs) at the University of Texas at Austin and the University of Texas at the Rio Grande Valley.
- Implement e-Procurement and Vendor Sales Reporting systems.
- Increase the DIR Executive Director's salary to better align with the salaries of similarly situated executive leaders in the field.
- Improve Texas.gov security.¹²¹

The 88th Legislative Session aligned customer eligibility for STS, and services and commodity items provided by DIR.¹²² This streamlined DIR-related statutes to allow for a clearer understanding of which customers may access which services or commodity items made

¹¹⁶ [Act of September 1, 2023, 88th Leg., R.S., ch. 67 \(S.B. 271\), § 1 \(to be codified at Gov't Code § 2054.603\).](#)

¹¹⁷ [Act of September 1, 2023, 88th Leg., R.S., ch. 1079 \(S.B. 621\), § 1 \(to be codified at Gov't Code § 2054.510\).](#)

¹¹⁸ [Act of September 1, 2023, 88th Leg., R.S., ch. 903 \(S.B. 1893\), § 1 \(to be codified at Gov't Code Chapter 620\).](#)

¹¹⁹ [Act of September 1, 2023, 88th Leg., R.S., ch. 473 \(H.B. 584\), § 1 \(to be codified as an amendment to Gov't Code § 2054.061\).](#)

¹²⁰ These bills from the most recent legislative session are discussed in more detail in Section VIII below.

¹²¹ [General Appropriations Act, 88th Leg., R.S., ch. 1170 \(H.B. 1\).](#)

¹²² [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\).](#)

available by DIR or through its programs.¹²³

As related to cybersecurity, the DIR Cybersecurity Incident Response Team (CIRT) acquired threat research capabilities including dark web analysis to help reduce the attack surface of Texas government entities. These improved cybersecurity threat hunting and intelligence capabilities allow the CIRT to better inform Texas government entities of system vulnerabilities, threat actor activities, and dark web activities.

The Cooperative Contracts program exceeded \$3 billion in revenue for the first time in the program's history. This monumental achievement represents not only a first for the program, but also a 9.2 percent increase in sales from the same period in fiscal year 2022.

After two decades of growth, the Information Security Forum (ISF), DIR's annual cybersecurity conference, is now regularly attended by 400-500 individuals with over 100 exhibitors. The ISF is now considered a premier cybersecurity event in Texas and is available at no cost to government attendees.

The Capitol Complex Telephone System VoIP migration efforts have successfully migrated 88 agencies to the new platform. The majority of the remaining customers requiring migration are at the Capitol and Capitol Extension buildings, which include the Texas House and Senate. DIR will begin work to transition the House and Senate at the conclusion of all legislative and special sessions in 2023 and with the authorization of House and Senate administrative offices. DIR projects a total estimated amount of 14,500 phones to be deployed by the conclusion of this modernization project.

DIR's STS programs continue to innovate and in 2023, DIR released the request for offer for Texas.gov Payment Services, and provided market notice of the upcoming procurements for multiple STS contracts.

Over 5.5 million users created accounts through TxT, representing 19 percent of the state's eligible population since it was officially launched in early 2022.

DIR and its staff were recognized for excellent work and innovation in the fields of information resources, cybersecurity, and technology throughout 2023:

- DIR was named a Top Workplace in the U.S. among employers with 150-499 employees for the second consecutive year.
- DIR received Top Workplace USA Culture Excellence 2023 awards in all five award categories, which include:
 - Purpose and Values, which celebrates organizations that have successfully communicated the company mission and integrated those aspirations into the

¹²³ [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\)\(to be codified at relevant sections of statute\).](#)

- culture;
- Work-Life Flexibility, which recognizes organizations that have built a culture that enables employees to meet the demands of their personal lives while maintaining high performance;
- Compensation and Benefits, which celebrates organizations that provide packages their employees believe are fair for the work being done and compared to others in the industry;
- Innovation, which recognizes organizations that have created a culture where new ideas are encouraged, which helps employees to reach their full potential and benefits performance; and
- Leadership, which celebrates organizational leaders who inspire confidence in employees and the company direction and listen to what matters most to employees and use that insight in decision making;
- DIR's Executive Director and Texas Chief Information Officer, Amanda Crawford, was named one of Government Technology's class of 2023 Doers, Dreamers, and Drivers.
- DIR's Chief People and Culture Officer, Lisa Jammer, received a State Leadership of the Year Award from StateScoop.
- The RSOC received a State IT Innovation of the Year Award from StateScoop.
- DIR was recognized by WeHireVets for having a workforce that is composed of more than 10 percent veterans.

IV. Policymaking Structure

a) Complete the following chart providing information on your policymaking body members.

Texas Department of Information Resources

Exhibit 4: Policymaking Body

Member Name	Term/Appointment Dates /Appointed by (e.g., Governor, Lt. Governor, Speaker)	Qualification (e.g., public member, industry representative)	City
Ben Gatzke Board Chair	6-year term, Appointed October 2016 Reappointed April 2017 Reappointed April 2023, Governor Appointed	Presiding Officer, Public Member (voting)	Fort Worth, TX
Mike Bell	6-year term, Appointed January 2018 Reappointed April 2023, Governor Appointed	Public Member (voting)	Spring, TX

Member Name	Term/Appointment Dates /Appointed by (e.g., Governor, Lt. Governor, Speaker)	Qualification (e.g., public member, industry representative)	City
Jeffrey W. Allison	6-year term, Appointed April 2022, Governor Appointed	Public Member (voting)	Houston, TX
Christopher “Stephen” Franke	6-year term, Appointed April 2022, Governor Appointed	Public Member (voting)	Dallas, TX
Stacey Napier	6-year term, Appointed June 2019, Governor Appointed	Institution of Higher Education (voting)	Austin, TX
Jeffrey Tayon	6-year term, Appointed April 2017 Reappointed January 2023, Governor Appointed	Public Member (voting)	Houston, TX
Kara Thompson	6-year term, Appointed June 2019, Governor Appointed	Public Member (voting)	Austin, TX
Cassie Brown (designee)	2-year term, Appointed February 2023, Statutory	Ex Officio Member (non-voting) Texas Department of Insurance	Austin, TX
Anh Selissen (designee)	2-year term, Appointed February 2023, Statutory	Ex Officio Member (non-voting) Texas Department of Transportation	Austin, TX
Maurice McCreary (designee)	2-year term, Appointed February 2023, Statutory	Ex Officio Member (non-voting) Texas Health and Human Services Commission	Austin, TX

b) Describe the primary role and responsibilities of your policymaking body.

The Texas Department of Information Resources (DIR) Board of Directors (DIR Board) is DIR’s governing board and policymaking body. In this role, the DIR Board is responsible for driving the overall strategy of DIR as an organization to ensure that Texas government entities can find and implement the most secure, reliable, and cost-effective technology available.

The DIR Board sets policy, adopts and repeals rules, appoints, and supervises the DIR Executive Director and the DIR Internal Auditor, approves contracts over \$1 million and major outsourced contracts, and establishes DIR’s strategic direction including new initiatives for—and service offerings under—DIR’s various programs.

c) How is the chair selected?

The Governor designates an appointed member of the DIR Board to serve as the presiding officer.

d) List any special circumstances or unique features about your policymaking body or its responsibilities.

The DIR Board comprises 10 board members. The Office of the Governor, with the advice and consent of the Texas Senate, appoints seven board members that serve for staggered six-year terms. One of the seven appointed board members must be employed by an institution of higher education as defined by Texas Education Code [Section 61.003](#).¹²⁴

The remaining three board member positions are filled by one of two groups of three statutorily identified, biennially rotating ex officio members. Only one group of ex officio members serve at a time. The first group's tenure begins on February 1 of every other odd-numbered year. The second group's tenure begins on February 1 of the odd-numbered years in which the first group's terms expire; the second group ends their term on February 1 of the next-odd numbered year.

The first ex officio member group includes:

- The Commissioner of Insurance;
- The Executive Commissioner of the Health and Human Services Commission; and
- The Executive Director of the Texas Department of Transportation.

The second ex officio member group includes:

- The Commissioner of Education (the Commissioner of the Texas Education Agency);
- The Executive Director of the Texas Department of Criminal Justice; and
- The Executive Director of the Parks and Wildlife Department.

A statutorily designated ex officio DIR Board member may, at their discretion, designate their role to an employee within the management or senior staff level of their state agency.

The DIR Board is statutorily required to define by rule what constitutes a major outsourced contract with regard to contracts the department executes with entities other than the state of Texas or a political subdivision of Texas.¹²⁵ These rules are codified in 1 Texas Administrative Code [Section 201.6](#), which defines a major outsourced contract as a contract that DIR executes with entities other than this state or a political subdivision of this state that is authorized under Government Code Subchapters I or L or Government Code Chapter 2170 or exceeds \$1

¹²⁴ [Tex. Educ. Code § 61.003](#).

¹²⁵ [Tex. Gov't Code § 2054.521](#).

million.¹²⁶

Contracts formed under Government Code Chapter 2054, [Subchapter I](#)¹²⁷ are State Electronic Internal Portal Project (Texas.gov Services and Texas.gov Payment Services) contracts. Contracts formed under Government Code Chapter 2054, [Subchapter L](#)¹²⁸ are Statewide Technology Services contracts necessary to support the Statewide Technology Centers.

The DIR Board is required to approve:

- DIR's award of any major outsourced contract;
- An amendment to a major outsourced contract if the amendment has significant statewide impact as defined by rule; or
- Any contract or amendment with a value expected to exceed \$1 million.¹²⁹

DIR Board members are subject to additional statutory conflict of interest requirements due to DIR's unique role in the IT and cybersecurity fields. To keep DIR procurement decisions free of real or perceived influence, Texas state law guides the activities of DIR Board members and DIR's Executive Director.

DIR Board members are prohibited by [Government Code Chapter 2054](#)¹³⁰ from:

- Being a person required to register as a lobbyist because of compensated activities for business entities or trade associations of business entities that have a substantial interest in the information resources technologies industry;¹³¹
- Acting as an officer, employee, or paid consultant of a business entity or trade association of business entities that have a substantial interest in the information resources technologies industries and that may contract with state government;
- Owning, controlling, or having more than a 10 percent interest in a business entity that has substantial interest in the information resources technologies industry and that may contract with state government;¹³²
- Receiving more than 25 percent of their income from a business entity that has substantial interest in the information resources technologies industry and that may contract with state government;¹³³

¹²⁶ [1 Tex. Admin. Code § 201.6\(c\)\(3\)\(A\)-\(B\).](#)

¹²⁷ [Gov't Code Chapter 2054, Subchapter I.](#)

¹²⁸ [Gov't Code Chapter 2054, Subchapter L.](#)

¹²⁹ [Gov't Code § 2054.522; see also 1 Tex. Admin. Code § 201.6\(d\).](#)

¹³⁰ [Gov't Code Chapter 2054.](#)

¹³¹ [Gov't Code § 2054.022\(a\)\(1\).](#)

¹³² [Gov't Code § 2054.022\(a\)\(3\).](#)

¹³³ [Gov't Code § 2054.022\(a\)\(4\).](#)

- Being interested in or connected with a contract or bid for providing information resources technology to a state agency;¹³⁴
- Being employed by a state agency as a consultant on information resources technologies at the same time as their term of service on the DIR Board;¹³⁵ and
- Accepting or receiving money or another thing of value from an individual, firm, or corporation to whom a DIR contract may be awarded;¹³⁶ however, this does not preclude a DIR Board member from being paid for services rendered to an agency.¹³⁷

A DIR Board member or the DIR Executive Director may not be the spouse of an officer, employee, or paid consultant of:

- A business entity that has—or a trade association of business entities that have—a substantial interest in the information resources technologies industry and that may contract with state government.

Voting and non-voting DIR Board members must complete a DIR-specific training program.¹³⁸ This training program requires DIR Board members to receive information on several categories outlined by statute that are pertinent to DIR, including an overview of DIR programs, finances, operations, and contract management processes. DIR Board members must complete this training within 180 days of the date on which the person takes office or begins serving as a member of the DIR Board.¹³⁹

This training program and its required categories of information are distinct from all other statutory trainings (such as the Office of the Attorney General and Comptroller of Public Accounts trainings discussed below) that DIR Board members must complete. Failure to complete another statutorily required training does not impact the DIR Board member's completion of this training program. DIR Board members must complete this training once and may do so by either reviewing the [DIR Board Training Guide](#) posted to DIR's website and confirming in writing their review of the DIR Board Training Guide or completing a virtual or an in-person training provided by DIR employees.

¹³⁴ [Gov't Code § 2054.022\(a\)\(5\).](#)

¹³⁵ [Gov't Code § 2054.022\(a\)\(6\).](#)

¹³⁶ [Gov't Code § 2054.022\(a\)\(7\).](#)

¹³⁷ See [Tex. Att'y Gen. Op. No. GA-0679 \(2008\)](#).

¹³⁸ [Gov't. Code § 2054.021\(f\)-\(g\).](#)

¹³⁹ *Id.*

e) In general, how often does your policymaking body meet? How many times did it meet in fiscal year 2021? In fiscal year 2022? Explain if the policymaking body met in-person or virtually during this time.

The DIR Board meets at least quarterly as required by law.¹⁴⁰ In addition to these quarterly meetings, the DIR Board is permitted by statute to meet at other times when the presiding officer determines that additional meetings are necessary.

During fiscal year (FY) 2021, the DIR Board met seven times:

1. October 1, 2020;
2. November 10, 2020;
3. January 28, 2021;
4. March 11, 2021;
5. May 06, 2021;
6. July 15, 2021; and
7. August 26, 2021.

During FY22, the DIR Board met four times:

1. October 28, 2021;
2. January 20, 2022;
3. April 28, 2022; and
4. August 25, 2022.

On March 16, 2020, [the Office of the Governor approved a request by the Office of the Attorney General](#) to temporarily suspend a number of open meetings laws, including the requirement for a presiding officer to be physically present at a specified meeting location. This decision authorized government bodies subject to the Open Meetings Act to meet in a fully virtual manner until the Office of the Attorney General sought—and the Office of the Governor approved their request—to lift the suspensions of the relevant sections of the Open Meetings Act. In alignment with this authorized suspension, the DIR Board convened all FY21 meetings virtually.

On June 30, 2021, [the Office of the Governor approved the Office of the Attorney General's request](#) to lift the Open Meetings Act suspensions beginning on September 1, 2021. Since the lifting of the Open Meetings Act suspensions, the DIR Board convenes all meetings with the presiding officer physically present at the location specified by its posted notice as required by statute; select DIR staff presenting to the DIR Board attend in person as well. All other DIR Board members, DIR staff, and the public may participate in the meetings virtually via videoconference or in person.

¹⁴⁰ [Gov't Code § 2054.027\(a\)](#).

f) Please list and describe all the training and training materials the members of the agency's policymaking body receive. How often do members receive this training or updated materials?

Open Government Training

Each appointed DIR Board member must complete two required trainings on open government that are published by the [Office of the Attorney General](#). The two separate required trainings provide detailed information on the Public Information Act and the Open Meetings Act, and board members must complete these trainings within 90 days after the date that they assume their responsibilities as a member of the DIR Board.¹⁴¹ DIR Board members must complete these trainings once and do not receive specific training updates from the Office of the Attorney General.

Purchasing and Contract Management Training

DIR Board members must complete an abbreviated training on purchasing and contract management that is developed by the [Comptroller of Public Accounts](#).¹⁴² This training details the ethical and professional responsibilities associated with state contracting. [Government Code Chapter 656](#) does not identify a specific deadline by which a governing body board member must complete this training.¹⁴³ DIR strongly recommends that DIR Board members complete this Comptroller of Public Accounts training no later than 90 days after beginning their term of service. DIR will accept a DIR Board member's notification of training completion up until their final day of service on the DIR Board. DIR Board members must complete this training once.

DIR Training

Voting and non-voting DIR Board members must also complete a DIR-specific training program.¹⁴⁴ This training program requires DIR Board members to receive information on several categories outlined by statute, including an overview of DIR programs, finances, operations, and contract management processes. DIR Board members must complete this training within 180 days after they take office or begin serving as a member of the DIR Board. This training program and its required categories of information are distinct from all other statutory trainings (such as the Office of the Attorney General and Comptroller of Public Accounts trainings discussed above) that DIR Board members must complete. DIR Board members must complete this training once and may do so by either reviewing the [DIR Board Training Guide](#) posted to DIR's website (and subsequently confirming in writing their review of the DIR Board Training Guide) or completing a virtual or in-person training provided by DIR

¹⁴¹ [Gov't. Code § 551.005](#); [Gov't. Code § 552.012](#).

¹⁴² [Gov't Code §§ 656.052, 656.053](#).

¹⁴³ [Gov't Code Chapter 656](#).

¹⁴⁴ [Gov't. Code § 2054.021\(f\)-\(g\)](#).

employees, a sample presentation of which may be provided upon request.

Cybersecurity Training

All DIR Board members must complete a state-certified cybersecurity training selected by DIR.¹⁴⁵ Through the selected program, DIR Board members develop information security habits and procedures that protect information resources as well as understand best practices for detecting, assessing, reporting, and addressing information security threats. This training must be completed through the state-certified cybersecurity training program selected by DIR at least once a year.

g) What information is regularly presented to your policymaking body to keep them informed about the agency's operations and performance?

The DIR Board meets at least quarterly as required by law.¹⁴⁶ DIR prepares comprehensive materials (the Board Book) containing all information necessary for the DIR Board to make any decision on a matter within its jurisdiction including documents brought before the DIR Board that are relevant to action items and other matters, quarterly and annual financial information, the slide deck presented during the DIR Board meeting, and the posted agenda. A designated DIR employee sends the Board Book for review to the DIR Board members in the preceding week before the DIR Board meeting.

In the preceding month of the quarterly or otherwise-scheduled DIR Board meeting, DIR hosts five separate DIR Board subcommittees, as detailed by subsection IV. (i) below, wherein the subcommittee reviews updates regarding matters within the subcommittee's jurisdiction prior to the open DIR Board meeting. During the respective subcommittee meetings, subcommittee members may ask DIR employees questions about the presented information; however, they are prohibited from taking action on issues presented before the subcommittee.

Beginning in 2019, DIR began sending occasional newsletters via email to the DIR Board. This newsletter provides updates on departmental programs and activities as well as other matters, issues, and events that impact—or are of relevance to—DIR. Following the conclusion of a legislative session, DIR includes updates on any legislative developments.

The DIR governing board presiding officer and Executive Director meet monthly to discuss issues of importance at DIR or any other matters that may otherwise impact—or are otherwise relevant to—DIR. In addition, when there is an urgent matter requiring immediate notification of the DIR presiding officer, the Executive Director or other senior staff disclose this information and any necessary and relevant details to the presiding officer.

The DIR Board is responsible for appointing an Internal Auditor, who reports directly to the DIR

¹⁴⁵ Gov't Code §§ [2054.519](#), [2054.5191](#).

¹⁴⁶ [Gov't Code § 2054.027\(a\)](#).

Board.¹⁴⁷ The Internal Auditor creates the DIR annual audit plan and presents this plan to the DIR Board for consideration; in addition, the Internal Auditor has the authority to report directly to the DIR Board any issue outside of the annual audit plan that requires the immediate attention of the DIR Board.¹⁴⁸ The DIR Board and the Internal Auditor may also meet outside of an open meeting as defined by the [Open Meeting Act, Government Code Chapter 551](#) to discuss issues related to fraud, waste, theft, and abuse.¹⁴⁹ The Internal Auditor provides regular updates to the DIR Board during the Audit, Finance, and Legal Subcommittee, as well as at regular board meetings in which there is an audit update for the entire board.

h) How does your policymaking body obtain input from the public regarding issues under the agency's jurisdiction? How is this input incorporated into the operations of your agency?

During open meetings, the DIR Board provides the opportunity for the public to address the DIR Board on an issue within its jurisdiction including agenda items and other matters before the DIR Board. In compliance with the [Open Meetings Act](#), the DIR Board announces its reasonable rules regarding public testimony at the beginning of each open meeting.

If an individual provides suggestions about DIR's operations during a public comment, the DIR Board may consider an action item to incorporate or implement it at a future DIR Board meeting where action regarding that item has been properly noticed under the Open Meetings Act.

The DIR Board is required to appoint a customer advisory committee, described below in section IV. (i), that includes a cross-section of members of the public and representatives from other government entities. In their roles as members of the customer advisory committee, public members must report to and advise the DIR Board on the status of DIR's delivery of critical statewide services.¹⁵⁰

i) If your policymaking body uses subcommittees or advisory committees to carry out its duties, fill in the following chart. For advisory committees, please note the date of creation for the committee, as well as the abolishment date as required by Texas Government Code, Section 2110.008.

In addition, please attach a copy of any reports filed by your agency under Texas Government Code Section 2110.007 regarding an assessment of your advisory committees as Attachment 28.

¹⁴⁷ [Gov't Code § 2054.038](#).

¹⁴⁸ [Gov't Code § 2054.038\(b\)-\(c\)](#).

¹⁴⁹ [Gov't Code § 2054.039](#).

¹⁵⁰ [Gov't Code § 2054.0331\(d\)](#); see also [1 Tex. Admin. Code § 201.5\(b\)\(3\)\(A\)-\(B\)](#).

Texas Department of Information Resources

Exhibit 5: Subcommittees and Advisory Committees

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
DIR Board Subcommittee – Audit, Finance, and Legal	4 Board Members	Provide oversight of DIR's Internal Auditor, financial matters, and legal issues, including DIR's administrative rules, and any other issues that the DIR Board considers appropriate. The DIR Board initially created this subcommittee to address statutory requirements that it maintain an audit subcommittee. As DIR's role in state government expanded, it became appropriate to include reports on financial and legal developments within the same meeting. On July 8, 2022, DIR renamed this subcommittee to address these additional functions.	Gov't Code § 2054.040	Creation: 9/1/2013 Updated Subcommittee Name and Purpose/Duties: 7/8/2022 Abolishment: N/A

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
DIR Board Subcommittee – Information Security	4 Board Members (3 voting, 1 Ex Officio)	Provide oversight of DIR's information security responsibilities, including monitoring statewide information security program assessments, participation, and progress, and reviewing information security issues and concerns impacting the State of Texas. Initially, DIR reported its information security updates during the Communications Technology Services and Information Security Subcommittee. However, as state leadership entrusted DIR with greater cybersecurity responsibilities and duties, the DIR Board found it necessary to update its subcommittee structure to ensure that more comprehensive and uninterrupted updates on how DIR is protecting the state's network daily through its Communications Technology Services Cybersecurity Operations team, and its efforts in assisting government entities in attaining the tools and knowledge necessary to prepare for and respond to their own cybersecurity incidents. All other aspects of the Communications Technology Services duties and responsibilities were removed to the jurisdiction of the Shared Technology Services and Communications Technology Services subcommittee, described below. In July 2022, the new Information Security Subcommittee was created.	Gov't Code Chapters 2054, 2059 (general authority)	Creation: 7/8/2022 Abolishment: N/A
DIR Board Subcommittee - Procurement and Contracting	4 Board Members (3 voting, 1 Ex Officio)	Provide oversight of DIR's procurement and contracting strategy, guidance related to procurement and contracting matters, and review the reliability and integrity of DIR's procurement and contracting program.	Gov't Code Chapter 2054 (general authority) Gov't Code § 2054.522(b)	Creation: 9/1/2013 Updated Subcommittee Name: 7/8/2022 Abolishment: N/A

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
DIR Board Subcommittee – Shared Technology Services and Communications Technology Services	4 Board Members (3 voting, 1 Ex Officio)	Provide oversight of DIR's Statewide Technology Center Services, which include the Data Center Services, Managed Application Services, and Managed Security Services programs, and Communications Technology Services (TEX-AN/CCTS). Review and monitor performance of and issues associated with both the Statewide Technology Center Services and TEX-AN and CCTS, including network updates, contracts, and customer purchases. Initially, DIR provided updates to its Board on the Texas.gov program and the Statewide Technology Services program, which included the Data Center Services, in two distinct subcommittees created explicitly for their respective purposes. In 2018, DIR began its transition to a Shared Technology Services program, that included within its scope of services the Texas.gov program, the Data Center Services offerings, the Managed Security Services, and the Open Data Portal. In July 2022, The Communications Technology Services were initially included as an element of the DIR Communications Technology Services and Information Security Committee as one aspect of the Communications Technology Services team duties include cybersecurity operations. Both the Shared Technology Services contracts and the Communications Technology Services are considered major outsourced contracts, as defined by the administrative code. In June 2022, the DIR Board determined that consolidating reporting to subcommittee members on DIR's major outsourced contracts and, by extension, the services provided by DIR and the awarded vendors under those contracts was a more effective means of providing updates.	Gov't Code § 2054.522 1 Texas Administrative Code § 201.6	Creation: 9/1/2013 Updated Subcommittee Name and Purpose/Duties: 7/8/2022 Abolishment: N/A

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
DIR Board Subcommittee - Strategic Initiatives	4 Board Members (All voting)	Provide oversight of DIR strategic initiatives, including statewide strategic oversight of DIR's statutorily mandated reporting on statewide strategic initiatives, DIR branding and program development initiatives, and data management issues associated with the Chief Data Officer's statutory responsibilities. This subcommittee was initially created as the Strategic Oversight Subcommittee. During subcommittee meetings, DIR reported to subcommittee members on its progress regarding statutorily mandated reports and strategic initiatives. As DIR expanded, however, so too did the needs of the Strategic Oversight Subcommittee to address various agency statewide responsibilities, such as the statutory duties of the Chief Data Officer, and DIR internal departments intended to support DIR's expanding strategic initiatives, such as the Program Development Office—now the Chief Experience Office. In July 2022, DIR rebranded the Strategic Oversight Subcommittee to the Strategic Initiatives Subcommittee to address the expanding needs.	Government Code Chapter 2054 (general authority)	Creation: 9/1/2013 Updated Subcommittee Name and Purpose/Duties: 7/8/2022 Abolishment: N/A

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
Customer Advisory Committee	Representatives of customers who receive services from each of the department's key programs, including state agencies with fewer than 100 employees, and the public. To the extent that is practicable, must represent a cross-section of DIR's customers, including representatives of primary customer groups, institutions of higher education, and the public.	Reports to and advises the board on the status of the DIR's delivery of critical statewide services	Gov't Code § 2054.0331 ; 1 Tex. Admin. Code § 201.5(b)	Creation: 9/1/2013 Abolished: N/A
Data Management Advisory Committee	Composed of: · Each Data Management Officer designated by a state agency. · DIR's Chief Data Officer.	Advises the board and DIR on establishing statewide data ethics, principles, goals, strategies, standards, and architecture. Provides guidance and recommendations on governing and managing state agency data and data management systems, including recommendations to assist Data Management Officers in fulfilling the duties assigned under Gov't Code § 2054.137. Establishes performance objectives for state agencies from this state's data-driven policy goals.	Gov't Code § 2054.0332	Creation: 06/14/2021 Abolishment: N/A

State Strategic Plan for Information Resources Management Advisory Committee	· Members are appointed by DIR's Executive Director with the approval of the DIR Board. · Membership must consist of at least 9 and not more than 21 members, which include officers or employees of state government but may not include a greater number of private sector representatives than public sector representatives. · Must include at least: · Two Information Resources Managers or a designee from Texas state agencies other than a university system or institution of higher education as defined by Tex. Edu. Code § 61.003. · One representative from a state university system or institution of higher education as defined by Tex. Edu. Code § 61.003. · One member of the public. · One representative from a local	Assist in the preparation of the state strategic plan that DIR's Executive Director is required to prepare pursuant to Government Code Chapter 2054, Subchapter E.	Gov't Code § 2054.091(d). 1 Tex. Admin. Code § 201.5(a)	Creation: on an as needed basis during the development of the State Strategic Plan. Abolishment: upon the completion of the State Strategic Plan.

Name of Subcommittee or Advisory Committee	Size/Composition /How are members appointed?	Purpose/Duties	Legal Basis for Committee (statute or rule citation)	Creation and Abolishment Dates
	government organization in the state that is knowledgeable about computing and/or telecommunications. - Three representatives from the computing and/or telecommunications industry. - One representative from a federal agency that is knowledgeable about computing and/or telecommunications.			

Currently, DIR mentions in our LAR and SSP that DIR has the advisory committees listed above. DIR has not included the three statutorily created committees (Customer Advisory Committee, Data Management Advisory Committee, State Strategic Plan Advisory Committee) in section 6.F.a (Advisory Committee Supporting Schedule) of DIR's LAR because those committees have had de minimis costs to the state. Moving forward, DIR will provide in section 6.F.a of the LAR a narrative that includes the evaluation required under Government Code Chapter 2110.

V. Funding

a) Provide a brief description of your agency's funding.

DIR is a cost recovery agency that is primarily funded by fees charged to customers for its offered services (Cooperative Contracts Clearing Fund, Communications Technology Services Telecommunications Revolving Account, Shared Technology Services – Statewide Technology Account, and Texas.gov Statewide Network Applications Account). As required by statute, the DIR Board of Directors reviews and approves all administrative fees proposed by DIR. The four main funds discussed above are all governed and outlined in Section (b) below, which includes the General Appropriations Act (GAA) riders that significantly impact DIR's budget, such as Rider 3 (DIR Clearing Fund Account), Rider 6 (Texas.gov Project and the Statewide Network

Applications Account), Rider 8 (Telecommunications Revolving Account), and Rider 9 (Statewide Technology Account).

Cooperative Contracts Funding

The revenue collected through the Cooperative Contracts program and deposited into the Clearing Fund Account amounted to approximately \$21.2 million in FY22. As of this report's writing, the amount for FY23 is projected to be \$23.3 million. Appropriations from this fund generally cover the administration of the Cooperative Contracts program, indirect administration, and cybersecurity services in accordance with Rider 11 (Fund Balance Limitations) of DIR's appropriations bill pattern. Rider 11 leverages the purchasing power of the state to negotiate indefinite delivery/indefinite quantity contracts, allowing customers to purchase as few or many of a given product without paying a premium for small purchases. DIR's Cooperative Contracts program is exclusively for information technology (IT) products and services. DIR negotiates and administers contracts with IT providers for products and services, including computer hardware, software, security hardware and software, networking and telecommunications equipment, IT staffing services, deliverables-based services, and technology-based training.

Communications Technology Services Funding

The Communications Technology Services program manages the Capitol Complex Telephone System (CCTS) and Texas Agency Network (TEX-AN). These programs provide voice, data, wireless, and internet services for agencies in the Capitol Complex, CCTS, and throughout the state. TEX-AN and CCTS revenue deposited into the Telecommunications Revolving Account amounted to approximately \$120.9 million in FY22. As of this report's writing, the amount for FY23 is projected to be \$115.5 million.

Shared Technology Services Funding

The Shared Technology Services (STS) program allows state and local government entities to outsource management of technology infrastructure services. These government customers receive the benefit of aggregated volume discounts by sharing technology services, while in turn receiving best-in-breed technology services from competitively procured industry-leading vendors. Data Center Services (DCS), which is a program of STS, provides secure connectivity to select public and private clouds designed around government security and disaster recovery requirements, offering flexible service tiers to meet differing needs and budgets. Joining the program allows customers to delegate infrastructure management while increasing their focus on delivering direct, mission-related value to their business users and clients. The revenue collected by STS and deposited to the Statewide Technology Account, excluding Texas.gov revenue, which has its own account in the GAA, amounted to approximately \$414.9 million in FY22. As of this report's writing, the amount for FY23 is projected to be \$478 million.

Texas.gov Funding

The revenue collected by Texas.gov and deposited into the Statewide Network Applications Account amounted to approximately \$76.8 million, net of payment processing fees, in FY22. As

of this report's writing, the amount for FY23 is projected to be \$79.6 million, net of payment processing fees. Texas.gov is the state's official website and trusted resource for Texans to access government information. Through Texas.gov, Texans can take care of government business such as driver's license and vehicle registration renewals, occupational licenses, permits, and more in an easy, secure, and user-friendly way. Appropriations from this fund cover the administration of the Texas.gov program including application development and maintenance costs in addition to customer support for the applications that process Texan transactions such as various license renewals, vital records, and vehicle registrations. The Texas.gov program is one of the STS programs provided by DIR. Texas.gov leverages enterprise-wide services and infrastructure components to provide solutions that meet or exceed state-mandated requirements regarding accessibility, security, privacy, and integration with the Texas Comptroller of Public Accounts. The appropriation to DIR is for estimated payments to service providers for application development, application maintenance, and customer support for the website.

General Revenue Funding

DIR receives General Revenue (GR) for cybersecurity services, which amounted to \$27.1 million in 2022. Those funds are allocated to:

- Multi-factor authentication (MFA);
- Regional Security Operations Centers (RSOCs);
- Endpoint detection and response (EDR) software for state agencies;
- Cybersecurity assessments; and
- Penetration tests for state agencies and institutions of higher education.

In the 88th Regular Session, the Texas Legislature appropriated \$4.6 million in GR for security services related to Texas.gov.

Federal Funding

DIR receives a minimal amount of federal funds via the Office of the Governor's Homeland Security Grant program for staffing related to the Cybersecurity Coordination team and its projects. This funding is further discussed in VII. Guide to Agency Programs - Cybersecurity.

b) List all riders that significantly impact your agency's budget.

Article I – DIR Bill Pattern

Clearing Fund Account

The Comptroller of Public Accounts shall establish in the state treasury the DIR Clearing Fund Account for the administration of cost recovery activities pursuant to authority granted under Chapters 771, 791, and 2157, Government Code. The account shall be used:

- As a depository for funds received as payments from state agencies, units of local government, and vendors for goods and services provided;
- As a source of funds for DIR to purchase, lease, or acquire in any other manner the services, supplies, software products, and equipment necessary for carrying out

DIR's duties to state agencies and units of local government from which DIR receives payment; and

- To pay salaries, wages, and other costs directly attributable to the services provided to state agencies and units of local government from which DIR receives payment; however, the maximum amount for all administrative costs to be applied to state agency receipts and local government receipts shall not exceed 2 percent per receipt.

Included in the amounts appropriated above in Strategies A.1.1, Statewide Planning and Rules; A.1.2, Innovation and Modernization; B.1.1, Contract Administration of IT Commodities and Services; C.1.1, Security Policy and Awareness; C.1.2, Security Services; D.1.1, Central Administration; D.1.2, Information Resources; and D.1.3, Other Support Services, are all balances not previously encumbered as of August 31, 2023, (estimated to be \$2,003,495) and revenues accruing during the 2024-25 biennium estimated to be \$17,113,335 in FY24 and \$20,275,298 in FY25 in revenue collected on or after September 1, 2023, appropriated from the sale of information technology commodity items out of Appropriated Receipts to the DIR Clearing Fund Account.

Any unexpended and unobligated balances as of August 31, 2024, out of appropriations made herein are appropriated for the same purposes to DIR for FY24 beginning September 1, 2024. For each fiscal year, if unexpended and unobligated balances and revenues are less than the amounts estimated by this rider, fund balances in the DIR Clearing Fund Account, authorized by Rider 11, Fund Balance Limitations, may be expended to address a shortfall, subject to the limitations on expenditures included in this rider.

DIR may not expend funds appropriated to DIR that exceed the total in Appropriated Receipts identified above for each fiscal year of the 2024-25 biennium without prior written approval from the Legislative Budget Board. DIR requesting the approval of the Legislative Budget Board shall submit in a timely manner the request along with adequate information for evaluating the request. Any additional information requested by the Legislative Budget Board must be submitted promptly and, in a manner prescribed by the Legislative Budget Board. The request shall be considered approved unless the Legislative Budget Board issues a written disapproval within 30 business days after the date the Legislative Budget Board staff concludes its review of the request and forwards the review to the Chair of the House Appropriations Committee, Chair of the Senate Finance Committee, Speaker of the House, and Lieutenant Governor. Any requests for additional information made by the Legislative Budget Board interrupt and restart the counting of the 30 business days.

Capital Purchases on Behalf of Other Government Entities

Any capital items related to information resources and telecommunications technologies purchased by DIR for use by other state agencies and government entities do not apply to DIR for the purpose of the capital budget rider limitations specified in Article IX, Transfers - Capital Budget, of the General Provisions of this Act.

Capital purchases made by DIR for DIR's internal use are subject to capital budget rider

limitations in Article IX, Transfers - Capital Budget, of the General Provisions of this Act.

Cash Flow Contingency

Contingent upon receipt of reimbursements from state agencies, other government entities, and vendors for direct services provided and procurements of goods or services, DIR may temporarily utilize additional General Revenue funds in an amount not to exceed the greater of 10 percent of projected revenue from telecommunications services provided under Government Code Chapter 2170, and revenue from the operation and management of Statewide Technology Centers under Government Code Chapter 2054, Subchapter L or \$4.0 million. These funds shall be utilized only for the purpose of temporary cash flow needs. The transfer and reimbursement of funds shall be made under procedures established by the Comptroller of Public Accounts to ensure that all borrowed funds are reimbursed to the Treasury on or before August 31, 2025.

Texas.gov Project and the Statewide Network Applications Account

The Comptroller of Public Accounts shall establish in the state treasury the DIR Statewide Network Applications Account for the administration of cost recovery activities pursuant to authority granted under Chapter 2054, Government Code.

Included in the amounts appropriated above in Strategies B.3.1, Texas.gov; D.1.1, Central Administration; D.1.2, Information Resources; and D.1.3, Other Support Services, are all balances not previously encumbered as of August 31, 2023, (estimated to be \$2,956,107) and revenues accruing during the 2024-25 biennium estimated to be \$45,838,757 in FY24 and \$48,753,379 in FY24 in revenue collected on or after September 1, 2023, appropriated from the operation and management of the Texas.gov State Electronic Internet Portal Project as provided by [Government Code Chapter 2054, Subchapter L](#), out of Appropriated Receipts and Interagency Contracts to the DIR Statewide Network Applications Account.

Any unexpended and unobligated balances remaining as of August 31, 2024, in the appropriation made herein are appropriated for FY24 beginning September 1, 2024, for the same purposes. For each fiscal year, if unexpended and unobligated balances and revenues are less than the amounts estimated by this rider, fund balances in the Statewide Network Applications Account, authorized by Rider 11, Fund Balance Limitations, may be expended to address a shortfall, subject to the limitations on expenditures included in this rider.

DIR may not expend funds appropriated to DIR that exceed the total in Appropriated Receipts and interagency contracts identified above for each fiscal year of the 2024-25 biennium without prior written approval from the Legislative Budget Board. DIR requesting the approval of the Legislative Budget Board shall submit in a timely manner the request along with adequate information for evaluating the request. Any additional information requested by the Legislative Budget Board must be submitted promptly and in a manner prescribed by the Legislative Budget Board. The request shall be considered approved unless the Legislative Budget Board issues a written disapproval within 30 business days after the date the Legislative Budget Board staff concludes its review of the request and forwards the review to the Chair of the House Appropriations Committee, Chair of the Senate Finance Committee, Speaker of the House, and

Lieutenant Governor. Any requests for additional information made by the Legislative Budget Board interrupt and restart the counting of the 30 business days.

Any funds received by DIR from other agencies or government entities for the purpose of adding or enhancing applications to—or functionality of—the Texas.gov project are appropriated to DIR and are exempted from the requirements of this rider for prior written approval from the Legislative Budget Board to expend such funds. DIR shall provide notification to the Legislative Budget Board as part of the quarterly Texas.gov financial reporting process and shall include the total amount estimated to be received in addition to describing the application or functionality to be added or enhanced.

DIR shall provide the Legislative Budget Board quarterly financial reports and expenditures on the Texas.gov project within 60 days of the close of each quarter.

Telecommunications, Statewide Technology Centers, and Texas.gov Capital Budget Purchases

Notwithstanding Article IX, §14.03, Transfers - Capital Budget, of this Act, DIR is hereby authorized to expend funds out of the Telecommunications Revolving Account, Statewide Technology Account, and Statewide Network Applications Account to acquire equipment, software, and maintenance that may be necessary to facilitate cost savings or technical advancements associated with the Capitol Complex Telephone System (CCTS), TEX-AN Statewide Telecommunications System, Statewide Technology Centers, or the Texas.gov State Electronic Internet Portal. DIR shall notify the Legislative Budget Board and the Governor 30 days prior to such acquisition.

Telecommunications Revolving Account

Included in amounts appropriated above in Strategies B.4.1, Communications Technology Services; C.1.2, Security Services; D.1.1, Central Administration; D.1.2, Information Resources; and D.1.3, Other Support Services, are all balances not previously encumbered as of August 31, 2023, (estimated to be \$4,662,550) and revenues accruing during the 2024-25 biennium estimated to be \$116,138,814 in FY24 and \$122,694,327 in FY25 in revenue collected on or after September 1, 2023, appropriated from telecommunications services as provided by Government Code Chapter 2170 out of Appropriated Receipts and Interagency Contracts to the Telecommunications Revolving Account.

Any unexpended and unobligated balances remaining as of August 31, 2024, in the appropriation made herein are appropriated for FY24 beginning September 1, 2024, for the same purposes. For each fiscal year, if unexpended and unobligated balances and revenues are less than the amounts estimated by this rider, fund balances in the Telecommunications Revolving Account, authorized by Rider 11, Fund Balance Limitations, may be expended to address a shortfall, subject to the limitations on expenditures included in this rider.

Included in amounts appropriated above is \$13,751,832 in FY24 and \$13,592,728 in FY25 in Appropriated Receipts and Interagency Contracts to the Telecommunications Revolving Account for the purpose of providing operating and administrative costs, excluding payments

to service providers for communications technology services for voice, data, wireless, and internet services for which DIR bills customer state agencies and government entities. DIR must notify the Legislative Budget Board to expend funds in excess of amounts identified in this rider for operating and indirect administrative costs. DIR may not expend funds in excess of 110 percent of the amounts identified in this rider for operating and indirect administrative costs without prior written approval from the Legislative Budget Board. DIR requesting the approval of the Legislative Budget Board shall submit in a timely manner the request along with adequate information for evaluating the request. Any additional information requested by the Legislative Budget Board must be submitted promptly and in a manner prescribed by the Legislative Budget Board. The request shall be considered approved unless the Legislative Budget Board issues a written disapproval within 30 business days after the date the Legislative Budget Board staff concludes its review of the request and forwards the review to the Chair of the House Appropriations Committee, Chair of the Senate Finance Committee, Speaker of the House, and Lieutenant Governor. Any requests for additional information made by the Legislative Budget Board interrupt and restart the counting of the 30 business days.

Annually, DIR shall report to the Legislative Budget Board, in a format prescribed by the Legislative Budget Board, actual spending by customer agencies and entities on telecommunications services.

Statewide Technology Account

In accordance with [Government Code Section 403.011](#), the Comptroller of Public Accounts shall establish within the state treasury an operational account called the Statewide Technology Account for all transactions relating to the operation and management of statewide technology centers.

Included in amounts appropriated above in Strategies B.2.1, Shared Technology Services; D.1.1, Central Administration; D.1.2, Information Resources; and D.1.3, Other Support Services, are all balances not previously encumbered as of August 31, 2023, (estimated to be \$3,720,515), and revenues accruing during the 2024-25 biennium estimated to be \$433,165,501 in FY24 and \$409,128,593 in FY25 in revenue collected on or after September 1, 2023, appropriated from the operation and management of Statewide Technology Centers as provided by [Government Code Chapter 2054, Subchapter L](#) out of Interagency Contracts and Appropriated Receipts to the Statewide Technology Account.

Annually, DIR shall report to the Legislative Budget Board, in a format prescribed by the Legislative Budget Board, actual spending by customer agencies and entities on shared technology services.

Any unexpended and unobligated balances remaining as of August 31, 2024, in the appropriation made herein are appropriated for FY24 beginning September 1, 2024, for the same purposes. For each fiscal year, if unexpended and unobligated balances and revenues are less than the amounts estimated by this rider, fund balances in the Statewide Technology Account, authorized by Rider 11, Fund Balance Limitations, may be expended to address a shortfall, subject to the limitations on expenditures included in this rider.

Included in amounts appropriated above is \$11,293,835 in FY24 and \$12,584,312 in FY25 in Appropriated Receipts and Interagency Contracts to the Statewide Technology Account for the purpose of providing operating and indirect administrative costs, excluding payments to service providers for data center services/shared technology services for which DIR bills customer state agencies and government entities. DIR must notify the Legislative Budget Board to expend funds in excess of amounts identified in this rider for operating and indirect administrative costs. DIR may not expend funds in excess of 110 percent of the amounts identified in this rider for operating and indirect administrative costs without prior written approval from the Legislative Budget Board. DIR requesting the approval of the Legislative Budget Board shall submit in a timely manner the request along with adequate information for evaluating the request. Any additional information requested by the Legislative Budget Board must be submitted promptly and in a manner prescribed by the Legislative Budget Board. The request shall be considered approved unless the Legislative Budget Board issues a written disapproval within 30 business days after the date the Legislative Budget Board staff concludes its review of the request and forwards the review to the Chair of the House Appropriations Committee, Chair of the Senate Finance Committee, Speaker of the House, and Lieutenant Governor. Any requests for additional information made by the Legislative Budget Board interrupt and restart the counting of the 30 business days.

Annually, DIR shall report all administrative costs collected and the administrative cost percentage charged to each state agency and other users of statewide technology centers as defined in Government Code Section 2054.380 to the Governor and Legislative Budget Board as directed in Government Code Section 2054.0346. The Legislative Budget Board and Office of the Governor shall consider the incremental change to administrative percentages submitted. Without the written approval of the Governor and the Legislative Budget Board, DIR may not expend funds appropriated to DIR if those appropriated funds are associated with an increase to the administrative cost percentage charged to users of the statewide technology centers and deposited to the Statewide Technology Account. The request to increase the administrative cost percentage shall be considered to be approved by the Legislative Budget Board unless the Legislative Budget Board issues a written disapproval within 30 business days after the date the Legislative Budget Board staff concludes its review of the request and forwards the review to the Chair of the House Appropriations Committee, Chair of the Senate Finance Committee, Speaker of the House, and Lieutenant Governor. Any requests for additional information made by the Legislative Budget Board interrupt and restart the counting of the 30 business days. In addition, by September 15 of each even-numbered year, DIR shall submit a report to the Legislative Budget Board detailing expended, budgeted, and projected costs for Data Center Services by participating agency. The report shall be in a format prescribed by the Legislative Budget Board.

Fund Balance Limitations

The following limitations apply to DIR funding:

- Before March 1 of each fiscal year, DIR shall prepare a report which reflects the amount of unexpended and unobligated balances carried forward in the DIR Clearing Fund, Telecommunications Revolving, Statewide Technology, and

Statewide Network Applications accounts, respectively from the previous fiscal year, and submit the report to the Office of the Governor, Legislative Budget Board, and the Comptroller of Public Accounts.

- For purposes of this section (Rider 11, Fund Balance Limitations), “agency” includes a state agency, institution of higher education, or local government entity that uses DIR IT commodity contracts, telecommunications, or Data Center Services, or is appropriated funds in this Act.
- For purposes of this subsection, “total revenue” means the total amount of administrative fees collected from users of DIR’s IT commodity contracts authorized by Government Code Chapter 2157. If unexpended and unobligated balances in the DIR Clearing Fund Account at the end of any fiscal year exceed 10 percent of total revenue processed through the account in that ending fiscal year, as defined in this subsection, the portion of the excess over 10 percent from all funding sources may be used in lieu of General Revenue for cybersecurity purposes as defined in Rider 12, Security Services to State Agencies and Institutions of Higher Education, of DIR’s bill pattern. Any General Revenue saved by this swap shall not be expended by DIR without prior written approval from the Legislative Budget Board for similar purposes. DIR shall report to the Legislative Budget Board quarterly on the use of excess fund balances for cybersecurity.
- For purposes of this subsection, “total revenue” means the total amount of gross revenue collected related to Telecommunications Services provided by DIR under [Government Code Chapter 2170](#). If unexpended and unobligated balances in the Telecommunications Revolving Account at the end of any fiscal year exceed four percent of total revenue processed through the account in that ending fiscal year, as defined in this subsection, the portion of the excess over the four percent funded from all funding sources may be used in lieu of General Revenue for cybersecurity purposes as defined in Rider 12, Security Services to State Agencies and Institutions of Higher Education, of DIR’s bill pattern. Any General Revenue saved by this swap shall not be expended without prior written approval from the Legislative Budget Board for similar purposes. DIR shall report to the Legislative Budget Board quarterly on the use of excess fund balances for cybersecurity.
- For purposes of this subsection, “total revenue” means the total amount of gross revenue collected related to Data Center Services provided by DIR under [Government Code Chapter 2054, Subchapter L](#). If unexpended and unobligated balances in the Statewide Technology Account at the end of any fiscal year exceed one percent of total revenue processed through the account in that ending fiscal year, as defined in this subsection, the portion of the excess over the one percent funded from all funding sources shall be returned to agencies, no later than May 1 of the following fiscal year. The excess returned to the agencies by DIR is appropriated to the agencies for expenditures consistent with the original funding source.

- For purposes of this subsection, “operating revenue” means the total amount of gross revenue collected related to the State Electronic Internet Portal, Texas.gov, provided by DIR under [Government Code Chapter 2054, Subchapter I](#), less the cost for payment processing services. If unexpended and unobligated balances in the Statewide Network Applications Account at the end of any fiscal year exceed four percent of operating revenue processed through the account in that ending fiscal year, as defined in this subsection, the portion of the excess over the four percent funded from all funding sources shall be transferred to the General Revenue Fund.
- The Comptroller of Public Accounts may prescribe accounting procedures and regulations to implement this section.
- The reimbursement requirements established by this section may be waived or delayed, either in whole or in part, by the Legislative Budget Board.
- DIR shall coordinate with the Legislative Budget Board on the development of a methodology to implement this section and a methodology to determine the source of funds used for agencies’ payments which are directly remitted to vendors for IT and telecommunications products and services.
- DIR shall require participating agencies to provide to DIR information regarding the specific funding sources from which agencies pay administrative costs charged for the use of DIR’s telecommunications and data center services respectively and as applicable.

Security Services to State Agencies and Institutions of Higher Education

Included in amounts appropriated above in Strategy C.1.2, Security Services, is \$31,654,157 in FY24 and \$29,984,157 in FY25 in General Revenue for the purpose of providing cybersecurity services to state agencies and institutions of higher education. Any unexpended and unobligated balances of these funds remaining as of August 31, 2024, are appropriated to DIR for FY24 beginning September 1, 2024, for the same purposes.

Texas.gov Security Improvements

Included in amounts appropriated above in Strategy B.3.1, Texas.gov, is \$4,568,248 from General Revenue in FY24 for the purpose of implementing security improvements on Texas.gov applications. Any unexpended or unobligated balances remaining as of August 31, 2024, are appropriated for the same purpose for FY24 beginning September 1, 2024.

Article IX Riders

Section 9.04. Texas.gov Project: Occupational Licenses

Each licensing entity not otherwise authorized to increase occupational license fees elsewhere in this Act may, as provided by [Government Code Section 2054.252\(g\)](#), increase the occupational license or permit fees imposed on the licensing entity’s licensees by an amount sufficient to cover the cost of the subscription fee charged by the Texas.gov Project to the licensing entity pursuant to Government Code Chapter 2054. Each licensing entity provided authority to impose a fee by [Government Code Section 2054.252\(g\)](#), and not otherwise

authorized to increase occupational license fees elsewhere in this Act, is appropriated the additional occupational license or permit fees in excess of the Comptroller of Public Accounts' biennial revenue estimate for 2024-25 for the sole purpose of payment to the Texas.gov contractor subscription fees for implementing and maintaining electronic services for the licensing entities. Each agency, upon completion of necessary actions to access or increase fees, shall furnish copies of board meeting minutes, an annual schedule of the number of license issuances or renewals and associated annual fee total, and any other supporting documentation to the Comptroller of Public Accounts. If the Comptroller of Public Accounts finds the information sufficient to support the projection of increased revenues, a notification letter will be issued, and the contingent appropriation made available for the intended purposes.

Section 9.05. Texas.gov Project: Cost Recovery Fees

Any cost recovery fees, excluding subscription fees as authorized under Government Code Chapter 2054, approved by DIR in relation to the Texas.gov Project as authorized under Government Code Chapter 2054, are appropriated to that agency from the fund to which the fee was deposited for the purpose of paying the costs associated with implementing and maintaining electronic services. Any unexpended balances remaining at the end of the fiscal biennium ending August 31, 2023, are reappropriated for the same purposes for the fiscal biennium beginning September 1, 2023.

Section 9.06. Prioritization of Cybersecurity and Legacy System Projects

Out of monies appropriated elsewhere in this Act and in accordance with Government Code Chapter 2054, DIR shall submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the Government Code Section 2054.571, to be considered for funding to the Legislative Budget Board by October 1, 2024. Agencies shall coordinate and cooperate with DIR for implementation of this provision.

Section 14.03. Transfers – Capital Budget

(H)(4): An agency may transfer appropriations into "data center consolidation," "data center services," or "shared technology services," as defined by Subsection (I)(2). An agency may transfer appropriations from "data center consolidation" or "data center services" or "shared technology services" as provided by [Government Code Section 2054.386](#) after obtaining the written approval of the Legislative Budget Board.

(L)(1): To provide for unanticipated shortages in appropriations made by this Act for FY24 for the payment of data center services costs, amounts identified elsewhere in this Act in FY25 for "data center consolidation," "data center services," or "shared technology services" may be transferred to FY24 to pay data center services costs.

(L)(2): "Data Center Consolidation," "Data Center Services," or "Shared Technology Services" for the purposes of this section are defined as services provided by DIR in accordance with Government Code Chapter 2054, including software licensing services, application services, security services, and public and private cloud services.

c) Show your agency's expenditures by strategy.

Texas Department of Information Resources

Exhibit 6: Expenditures by Strategy – Fiscal Year 2022 (Actual)

Goal/Strategy	Amount Spent	Percent of Total	Contract Expenditures Included in Total Amounts
A.1.1 – Statewide Planning and Rules	\$1,337,606	0.22%	\$132,226
A.1.2 – Innovation and Modernization	\$795,037	0.13%	\$364,760
B.1.1 – Contract Administration of IT Communications and Services	\$4,779,617	0.80%	\$1,809,604
B.2.1 – Shared Technology Services	\$410,146,325	68.72%	\$406,701,230
B.3.1 – Texas.gov	\$41,019,433	6.87%	\$38,343,377
B.4.1 – Communications Technology Services	\$108,045,465	18.10%	\$102,685,092
C.1.1 – Security Policy and Awareness	\$921,560	0.15%	\$625,985
C.1.2 – Security Services	\$23,920,117	4.01%	\$21,538,909
D.1.1 – Central Administration	\$2,843,269	0.48%	\$266,427
D.1.2 – Information Resources	\$2,556,688	0.43%	\$1,204,456
D.1.3 – Other Support Services	\$509,316	0.09%	\$90,288
Total	\$596,874,433	100.00%	\$573,762,355

d) Show your agency's source of revenue. Include all local, state, and federal appropriations, all professional and operating fees, and all other sources of revenue collected by the agency, including taxes and fines.

Texas Department of Information Resources

Exhibit 7: Sources of Revenue – Fiscal Year 2022 (Actual)

Source	Amount
DIR Clearing Fund Account	\$21,179,757
Telecommunications Revolving Account	\$120,915,767
Statewide Technology Account	\$414,870,768
Statewide Network Applications Account	\$76,814,968
General Revenue	\$27,102,832
Federal Funds	\$475,330
Total	\$661,359,422

e) If you receive funds from multiple federal programs, show the types of federal funding sources.

Texas Department of Information Resources

Exhibit 8: Federal Funds – Fiscal Year 2022 (Actual)

Type of Fund	State/Federal Match Ratio	State Share	Federal Share	Total Funding
Homeland Security Grant 97.067.0002	NA	\$475,330	N/A	\$475,330
Total		\$475,330	N/A	\$475,330

f) If applicable, provide detailed information on fees collected by your agency. Please explain how much fee revenue is deposited/returned to the General Revenue Fund and why, if applicable.

Texas Department of Information Resources

Exhibit 9: Fee Revenue – Fiscal Year 2022

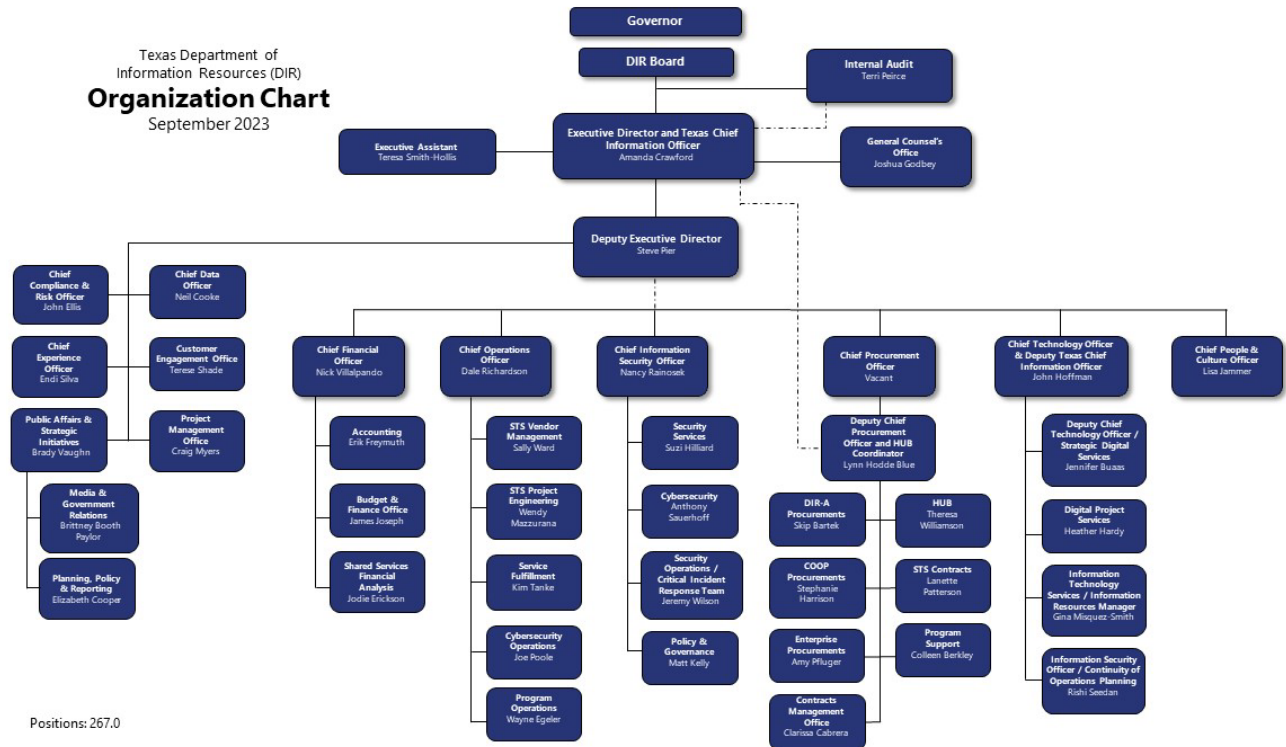
Fee Description/ Program/ Statutory Citation	Current Fee	Fees Set by Statute or Rule?	Statutory Maximum or Minimum, if applicable	Number of Persons or Entities Paying Fee	Fee Revenue	Where Fee Revenue is Deposited (e.g., General Revenue Fund)
Cooperative Contracts Fee/Cooperative Contracts program/Government Code § 2157.068(d)	0.69% Average	Authorized by Statute, set by DIR Board	2% maximum set in General Appropriations Act	3,433	\$21.2 million	Other Funds – DIR Clearing Fund Account
Shared Technology Services Fee/Shared Technology Services Program/Government Code § 2054.380	2.95%	Authorized by Statute, set by DIR Board	2.95% set in General Appropriations Act	146	\$414.9 million (gross revenue)	Other Funds – Statewide Technology Account
Texas.gov Convenience Fees and Subscription Fees/Texas.gov Program/Government Code § 2054.252(e) and 2054.2591	Various, based on service	Authorized by Statute, set by DIR Board	Not applicable	57.4 million constituent transactions	\$76.8 million, net of payment processing fees	Other Funds – Statewide Network Application Account

Fee Description/ Program/ Statutory Citation	Current Fee	Fees Set by Statute or Rule?	Statutory Maximum or Minimum, if applicable	Number of Persons or Entities Paying Fee	Fee Revenue	Where Fee Revenue is Deposited (e.g., General Revenue Fund)
TEX-AN Fees/Communications Technology Services /Government Code § 2170.057(a)	Various, based on service	Authorized by Statute, set by DIR Board	Not applicable	898 billed customers and 3215 customers through GoDirect Contracts	\$110.8 million (gross revenue)	Other Funds – Telecommunicatio ns Revolving Account
CCTS Fees/Communications Technology Services/Government Code § 2170.057(a)	Various, based on service	Authorized by Statute, set by DIR Board	Not applicable	95	\$10.1 million (gross revenue)	Other Funds – Telecommunicatio ns Revolving Account

VI. Organization

- a) Provide an organizational chart that includes major programs and divisions and show the number of FTEs in each program or division. Detail should include, if possible, division heads with subordinates, and actual FTEs with budgeted FTEs in parenthesis.

Figure 4 Organization Chart



Please see the full organization chart as an attachment to this report.

Entering FY24, DIR reorganized the agency's organizational structure to better reflect how DIR provides service to Texas and improve transparency, internal communications, and coordination. This improved structure supports the 2023 strategic vision of refining processes to improve customer and employee experiences, continuing to set the standard for government technology leadership and excellence, and providing Texans with a positive and streamlined experience of government.

b) Fill in the chart below listing the agency's headquarters and number of FTEs and, if applicable, field or regional offices.

Texas Department of Information Resources

Exhibit 10: FTEs by Location – Fiscal Year 2023¹⁵¹

Headquarters, Region, or Field Office	Location	Number of Budgeted FTEs FY23	Number of Actual FTEs (as of SER submission)
William P. Clements Building	Austin	179	173
Network Security Operations Center	Austin	57	48
Sam Houston Building	Austin	13	12
San Angelo Data Center	San Angelo	1	1
Total		250	234

c) What are your agency's FTE caps for fiscal years 2021-25?

Figure 5 FTE Caps for FY21 to FY25

Year	FTE Cap
2021	208
2022	228
2023	228
2024	267
2025	267

d) How many temporary or contract employees did your agency have in fiscal year 2022? Please provide a short summary of the purpose of each position, the amount of expenditure per contract employee, and the procurement method of each position.

Figure 6 Contracted Workforce by Quarter

Contract Workforce	Quarter 1	Quarter 2	Quarter 3	Quarter 4	Average
Active Contractors (Headcount)	11.0	16.0	13.0	10.0	12.5
FTE Impact Contractors	8.9	8.0	7.0	8.4	8.1

¹⁵¹ Full-time Equivalent (FTE) counts are current as of August 2023.

Figure 7 Temporary or Contract Employees

Program	Contract	Procurement Method	Expenditure	Purpose	Headcount
Agency Administration - Accounting	DIR-CPO-4642	Direct purchase – set aside	\$125,397	General ledger accounting support	1
	DIR-CPO-4642	Direct purchase – set aside	\$62,978	Telecom AR/AP accounting support and data analysis	1
Agency Administration - Information Technology Services	DIR-CPO-4549	Request for Quote/pricing	\$792,746	Database administration, data modeling, applications development, and support of the Data Optimization project.	5
	DIR-CPO-4612	Request for Quote/pricing	\$55,713	IT Help Desk support	1
	DIR-CPO-4688	Request for Quote/pricing	\$7,584	Salesforce programming support	1
	DIR-TSO-4612	Request for Quote/pricing	\$46,752	IT Help Desk support	2
	DIR-CPO-4642	Request for Quote/pricing	\$13,940	Quality assurance testing and web content management	1
	DIR-TSO-4667	Request for Quote/pricing	\$5,925	Programming analysis related to the Data Optimization project	1
	DIR-TSO-4682	Request for Quote/pricing	\$47,716	Software development	1
Cybersecurity	DIR-TSO-4518	Request for Quote/pricing	\$157,018	Cloud security risk assessment	1
	DIR-CPO-4642	Request for Quote/pricing	\$32,761	Cybersecurity team support	1
	DIR-CPO-4642	Request for Quote/pricing	\$51,015	Cloud security risk assessment specialist	1
IT Procurement and Contracting	DIR-CPO-4642	Direct purchase – set aside	\$109,787	Contract administration support	1
	DIR-TSO-4529	Request for Quote/pricing	\$143,867	Contract management support	1
	DIR-TSO-3531	Request for Quote/pricing	\$215,895	Contract management, procurement leadership	1
	DIR-CPO-4642	Request for Quote/pricing	\$37,604	Contract administration support	1
	DIR-TSO-4617	Request for Quote/pricing	\$21,153	Contract administration support	1

e) List each of your agency's key programs or functions, along with expenditures and FTEs by program.

Texas Department of Information Resources

Exhibit 11: List of Program FTEs and Expenditures — Fiscal Year 2022

Program	Actual FTEs FY22 (Including Contractors)	Budgeted FTEs FY23	Actual Expenditures FY22	Budgeted Expenditures FY23
Agency Administration	60.2	71.4	\$10,991,308	\$13,222,322
Cybersecurity	20.3	36.0	\$24,837,648	\$56,152,497
Shared Technology Services	23.2	21.3	\$408,593,135	\$381,662,745
Communications Technology Services	41.9	44.6	\$105,071,519	\$101,061,310
Data Management	3.6	4.0	\$479,128	\$586,062
Texas.gov	5.6	8.7	\$40,656,031	\$42,436,768
Technology Planning and Innovation	12.2	10.9	\$1,505,474	\$2,805,290
IT Procurement and Contracting	46.6	53.1	\$4,740,190	\$6,662,462
Total	213.6	250.0	\$596,874,433	\$604,589,456

Guide to Agency Programs

The following sections describe each key agency function for the Texas Department of Information Resources (DIR). As described by this section, DIR provides many different services to its customers, a term that includes different public sector entities. However, while these services are different, they are not disparate, as all of DIR's functions, including cybersecurity, communications technology services, and procurement of IT commodities inform the greater notion of information technology in the state of Texas.

VII. Guide to Agency Programs – Agency Administration



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by **leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.**

a) Provide the following information at the beginning of each program description.

Name of Program or Function: Agency Administration

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Amanda Crawford

Statutory Citation for Program:

Specific Requirements for DIR

[Government Code Chapter 2054, Information Resources Management Act](#)

[Government Code Chapter 2055, Electronic Grant System](#)

[Government Code Chapter 2059, Texas Computer Network Security System](#)

[Government Code Chapter 2155, Purchasing: General Rules and Procedures](#)

[Government Code Chapter 2157 Purchasing: Purchase of Automated Information Systems](#)

[Government Code Chapter 2170, Telecommunications Services](#)

[Government Code Chapter 2262, Statewide Contract Management](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.

Exceptional
Total Experience



Operational
Excellence



The objective of DIR's Agency Administration function is to provide leadership and support to the daily operations of the agency and the mission of DIR.

The Agency Administration function currently includes the Executive Director and Deputy Executive Director, Office of General Counsel, Chief Experience Office, Chief Financial Office, DIR's internal Information Security Officer, Information Technology Services, Internal Audit, Chief Compliance and Risk Officer, People and Culture Office, Project Management Office, and the Office of Public Affairs and Strategic Initiatives.

Executive Director and Deputy Executive Director

DIR's Executive Director manages all agency functions and priorities. The Executive Director is accountable for all agency functions and directs all agency initiatives and budgets; implements board policies and directives; and represents the agency and DIR's Board of Directors in front of policymakers and stakeholders. DIR's Executive Director is statutorily designated as the State of Texas' Chief Information Officer (CIO).

As state CIO, the Executive Director guides Texas' IT policy by evaluating industry best practices and communicating them to other state agencies, the Office of the Governor, and the Texas Legislature. The CIO also identifies and understands current technology trends and the needs of state entities to allow DIR to better identify offerings that meet the future technology and cybersecurity needs and expectations of Texas government and Texans. Additionally, the CIO represents the state nationally as an IT leader and steward of the Texas model of providing IT services. Due to the CIO's extensive participation in national conversations about IT and cybersecurity, Texas has become a nationally recognized leader in these fields. Other states have even adopted or are beginning to adopt the Texas model due to the CIO's consultative and collaborative work, which yields more opportunities for Texas, including better pricing, more vendor competition for Texas solicitations, and increased sales through DIR's Cooperative Contracts program, resulting in greater revenue for the state.

The Deputy Executive Director supports the Executive Director, serving as the Executive Director's designee when they are unavailable. The Deputy Executive Director assists with the execution of agency priorities and manages divisions focused on external relations, policy, outreach, and customer experience.

Office of General Counsel

The Office of General Counsel advises the DIR Board and Executive Director on legal issues and provides legal counsel and general legal support for DIR staff functions, including all DIR programs, contracts, and procurements, to ensure compliance with statutes and the Texas Comptroller of Public Account's Texas Procurement and Contract Management Guide.

For all DIR program areas, the Office of General Counsel: drafts, negotiates, reviews, and interprets contracts and other agreements; supports the procurement process; coordinates litigation with the Office of the Attorney General; coordinates the rulemaking process; and addresses legal matters related to agency administration, human resources, employment law, and labor matters. The Office of General Counsel also provides training for DIR's Board, agency new hires, and existing employees.

In addition to these general roles, the Office of General Counsel also houses several specific duties including:

- DIR's Privacy Officer, who provides legal advice, guidance, and training on privacy matters, reviews all DIR contracts and procurements that may involve or implicate personally identifiable information to ensure the protection of constituent data by vendors or third parties, coordinates with DIR's Information Security Officer to

establish an internal incident response plan, assists other agencies with incident response when a data breach occurs, and ensures agency policies and procedures comply with state and federal privacy laws and adhere to best practices in the privacy field. The Privacy Officer also participates in DIR's artificial intelligence (AI) initiatives to ensure the consideration of privacy principles as the state looks to incorporate AI into its business operations;

- The DIR Ethics Office, which provides legal advice and counsel to DIR employees and the DIR Board on ethics questions to ensure DIR's compliance with state laws and (advisory) opinions from other state agencies regarding ethics issues; and
- The Public Information Office, which manages public information requests and processes them in accordance with the requirements of [Government Code Chapter 552](#).

Chief Experience Office

The Chief Experience Office (CXO) oversees communications and outreach for DIR, develops and implements strategies to improve customer experience for agency programs, and ensures that the agency communicates the value of DIR programs with holistic, unified, and consistent messaging. The CXO helps break down silos of customer communication across DIR programs so that external communications are clear and targeted toward intended audiences. As DIR implements solutions to help government entities transform their technology environment, the CXO promotes and clarifies information on those solutions to customers that need or who may otherwise be interested in the use of them.

The CXO is the driving force behind DIR's external visibility through its successful management of DIR's digital presence, social media, campaigns, and events, including the design and content of DIR's website, and its coordination of DIR presentations, awards, and attendance at major conferences. The CXO also facilitates DIR's statutorily required Customer Advisory Committee.

The team is responsible for agency branding and ensures the effectiveness of this effort by planning the layout, design, illustration, content, and production of agency communication products, ensuring the accuracy, consistency, and effectiveness of agency materials, and coordinating outreach decisions for Texas.gov marketing initiatives. In furtherance of this goal, the CXO oversees and selects the materials for the distribution of agency communication products while also developing and distributing newsletters for internal employees and external customers, customer satisfaction surveys, and customer reports. The CXO develops customer experience strategies for understanding the needs of the customers, partnering with agency divisions to establish the agency's customer experience strategy.

Chief Financial Office

The Chief Financial Office (CFO) has managed the agency's growth from a \$261 million budget in 2013 to a \$467 million budget in 2023, all while maintaining approximately 30 current full-time employees. In FY22, through the Shared Services Financial Analysis, Telecom Accounts Receivable/Payable, and General Ledger departments, the Chief Financial Office managed

approximately \$557.6 million in shared technology and telecommunications services consumed by DIR customers by negotiating financial terms and prices, monitoring functions specific to contract financial terms and conditions, disputing vendor charges when necessary or appropriate, and remitting payments to service providers. The Chief Financial Office effectively manages financial issues associated with DIR contracts and vendors so that DIR customers can focus mission critical information technology implementation and operations.

Information Security Officer

DIR's Information Security Officer (ISO) is responsible for the statutory tasks required of designated Information Security Officers by Government Code Section 2054.136 and is governed by [1 Texas Administrative Code Chapter 202](#).

DIR's ISO is the employee responsible for internal information security efforts. The ISO maintains DIR's compliance with all applicable cybersecurity laws and control requirements for DIR, is responsible for the agency's strategic security roadmap, and works with all DIR divisions to assess, identify, and resolve any vulnerabilities to or in DIR systems or infrastructure. The ISO also works with agency staff to reduce information security and privacy risks and ensure that security is considered in all appropriate phases of internal IT system development and that DIR requires secure access to agency information. Should DIR be the subject of a security or privacy incident, the ISO must respond effectively and in a timely manner to executive management, impacted business units, and all other DIR employees responsible for recovery and mitigation.

In addition, the ISO oversees all agency continuity of operations planning, including any additional federal and state requirements, and serves as a liaison with federal, state, and local government to coordinate continuity and restoration activities, plans, and services. The ISO reviews and evaluates DIR's continuity of operations plans, test outcomes, risk assessments, proposed processes, systems, and preventative measures. The ISO is also one of DIR's liaisons with the Texas Division of Emergency Management and helps coordinate DIR's response for Emergency Support Function activations related to non-cybersecurity incidents.

Information Technology Services Team

The Information Technology Services (ITS) team supports DIR's mission by providing software development, systems configuration, and technology maintenance and support for all devices and systems infrastructure, to ensure the safe and secure use of DIR systems. The ITS team furthers the agency's vision and strategic focus by planning for growth, installing systems, and supporting and maintaining all IT systems at DIR, including computing and mobile devices. The ITS team also manages the agency's infrastructure, maintaining, upgrading, and troubleshooting at each of the DIR offices in Austin.

Internal Audit

Internal Audit provides independent, objective assurance and consulting services designed to add value to and improve DIR's operations. Annually, Internal Audit assesses agency risks and develops an audit plan for Board approval. Throughout the year, Internal Audit monitors agency activities by providing risk-based and objective assurance, advice, and insight, serving

as DIR's liaison for external auditors and Project Manager for audits by external firms selected to perform the audits identified in the annual audit plan.

Chief Compliance and Risk Officer

Technology's rapid, daily growth and overall importance in contrast with Texas' biennial legislative cycle create unique compliance challenges to DIR's role as the information technology and cybersecurity agency for the state. Not only has technology changed rapidly over recent years, but DIR itself has experienced rapid expansion in the number of customers it serves, the quantity, value, and complexity of the contracts it procures and manages, and the overall complexity of goods and services that public entities are acquiring through DIR contracts. Furthermore, in recent years, Texas has faced increasing challenges related to cybersecurity, including the growing need to balance efficient government operations with an enhanced awareness of Texans' privacy rights.

Under these circumstances, DIR recognized the need of devoting significant resources to constantly review its business practices and monitor the growth in DIR's risk portfolio from changing technology, complex cybersecurity and privacy considerations, and the need to comply with laws that are frequently outdated when considering the pace at which technology changes. To assist with this task, DIR employs a Chief Compliance and Risk Officer who has legal expertise. The Chief Compliance and Risk Officer is tasked with constant analysis of both policies and procedures, as well as everyday operational decision-making, to identify compliance challenges and risks that could jeopardize DIR's programs from achieving their statutory goals.

The Chief Compliance and Risk Officer helps DIR staff develop and execute policies, standard operating procedures, and business strategies that prioritize excellence in compliance with legal and ethical standards. The Chief Compliance and Risk Officer is also responsible for analyzing DIR's risk portfolio, risk tolerance, and risk culture to develop insights that empower DIR to make more calculated business decisions.

DIR created this role because of DIR's commitment to compliance and addressing emerging risks related to DIR's growth rate in both scope and volume of functions. The Chief Compliance and Risk Officer supports the Internal Auditor, ensuring that leadership complies with auditor requests, monitors, and follows up on remediation and audit findings, and ensures that management considers and acts on risks or compliance deficiencies identified by the Internal Auditor.

People and Culture Office

DIR is an IT agency powered by its people. To support this mission, the People and Culture Office leads the vision, strategy, development, and execution of DIR's talent and culture management programs to advance the agency's mission, vision, and core value statements. The key functions of the People and Culture Office include headcount planning, recruitment and selection, onboarding, performance management, learning and development, and internal mobility (including career planning, facilities management, workplace safety, fleet management, personal wellbeing, HR records management, and total rewards). The Office fosters a dynamic

culture that attracts, develops, and retains top talent through transparent communications, accountability, mutual respect, and shared mission.

The People and Culture Office also leads the agency's adoption of, education on, and compliance with state, federal, and local employment laws and regulations while also incorporating industry best practices to recruit and retain top IT talent.

Project Management Office

The Project Management Office supports DIR's execution and the management of its portfolio of projects. To accomplish this, the Project Management Office focuses on three areas to assist DIR's programs in achieving the agency's goals.

- **Project Management Methodology:** To comply with statutory and administrative code requirements and industry best practices, every project requires administration, although such administration may be managed by Project Managers within the division executing the project. The Project Management Office develops and maintains the Project Management Essentials, a common project methodology, that must be employed for all agency projects that do not meet the criteria for a Major Information Resources Project (MIRP), as discussed in the Technology Guidance and Innovation Function. The Project Management Essentials consists of tools, templates, and best practices that empower DIR employees to be more efficient and effective in project delivery, regardless of project size or complexity. Project Management Essentials is available on the DIR website¹⁵² so other state and local entities may use it to achieve their core missions through successful project delivery.
- **Project Management Services:** The Project Management Office provides staff to fulfill project management requirements, especially when a project is deemed large, complex, or significant enough to warrant the Project Management Office's involvement. The Project Management Office also offers consultive services and administrative support on projects.
- **Project Portfolio Management and Governance:** The Project Management Office assists DIR leadership with their management of the agency's project portfolio. This includes facilitating the initiation, approval, and prioritization of projects in addition to reporting on the portfolio of projects at DIR.

Office of Public Affairs and Strategic Initiatives

The Office of Public Affairs and Strategic Initiatives serves as DIR's liaison with the Texas Legislature, the Office of the Governor, other state agencies and government entities, various

¹⁵² Project Management Essentials is available at <https://dir.texas.gov/technology-policy-and-planning/digital-project-services/project-management-essentials-pm-essentials>.

stakeholder groups, and the media. The Office of Public Affairs and Strategic Initiatives communicates clear, accurate, and helpful information to educate state leadership and the media about technology, cybersecurity, and DIR and its programs. The Office also oversees legislative budget matters, strategic reporting, agency legislative priorities, and interactions with the Legislature and other agencies, including coordinating subject matter experts to provide testimony before the Legislature and responses to legislative inquiries. The Office of Public Affairs and Strategic Initiatives tracks and monitors legislation during legislative sessions and coordinates the agency's implementation of any legislation passed that impacts DIR.

In addition to these duties, the Office of Public Affairs and Strategic Initiatives works with other DIR divisions to produce statutorily required reports, including DIR's Legislative Appropriations Requests, the state's strategic IT plan, biennial performance reports, and the agency's strategic plan. In its role as the media point of contact, the Office of Public Affairs and Strategic Initiatives responds to press inquiries and drafts documents, speeches, talking points, and communications to other agencies and the Legislature.

c) What information can you provide that shows the effectiveness and efficiency of this program or function?

The effectiveness of the Agency Administration function is reflected in the overall performance of the agency, as discussed in Section II. (h). See below for additional information that is relevant to the specific groups within the Agency Administration function and not captured by other sections.

Office of General Counsel

The Office of General Counsel provides legal advice, counseling, and training to DIR divisions and departments. This includes providing regular employment counsel to DIR's People and Culture Office, ethics training to each new employee joining the DIR team, and ongoing ethics training and advice as needed to agency managers, employees, and DIR board members.

The Office of General Counsel plays an extensive role in the negotiation and review of enterprise, Cooperative Contracts, and internal DIR contracts and procurements to ensure that awarded contracts comply with state and federal law and protect the state's interests and resources in agreements with third parties. As Texas' information technology and cybersecurity agency, DIR has a vested interest in ensuring the application of privacy best practices; the Office of General Counsel supports this effort by reviewing contracts to ensure that Texans' personal information collected either by the state or pursuant to a contract is adequately protected.

DIR's Shared Technology Services contracts are complex, requiring multiple amendments a year. DIR's Office of General Counsel supports the Chief Procurement Office teams in amending these contracts, ensuring that the proposed amendments are within the scope of the contract award and compliant with law. In addition to the Shared Technology Services (STS) contracts, the Office also supports the dozens of internal contracts that DIR enters into each year and the more than 1,000 contracts that DIR has procured, negotiated, and amended across both the

Cooperative Contracts and Communications Technology Services Programs.

The Office of General Counsel is critical to the success of DIR's negotiations teams and provides necessary legal insight during contract negotiations. Of the many contract negotiations of which the Office of General Counsel is a part, more than 10 percent are for contracts with Fortune 100 companies; DIR negotiates many contracts with Fortune 500 companies, as well. During the last two years, DIR procured and negotiated over 500 contracts. In FY22, these contracts accounted for nearly \$3.5 billion in sales. Over 275 of DIR's contracts have sales over \$1 million across the biennium.

The Office of General Counsel also houses the Public Information Office and manages and processes public information requests in compliance with [Government Code Chapter 552](#).¹⁵³ From June 1, 2022, to June 30, 2023, DIR received 880 public information requests and released 2,259 individual documents. DIR works extensively with its requestors to ensure that they receive the documents they are seeking, making sure to clarify when clarity is required. Due in no small part to this collaborative effort with its requestors, DIR only submitted 14 of its 880 received public information requests to the Office of the Attorney General (OAG) for a determination as to whether DIR must or may withhold responsive information subject to a confidentiality exception in the Public Information Act. DIR's briefings asserted confidentiality of responsive information under the network security, deliberative process, and attorney-client exceptions. In addition, DIR provided notice to 109 third parties of a public information request to which the third party's confidential information was responsive with almost all DIR submissions to the OAG requiring a notice of at least one third party.

Chief Experience Office

DIR's mission is to provide innovative and cost-effective technology and cybersecurity solutions for its government customers. DIR would be limited in fulfilling that mission without outreach efforts that promote DIR services and initiatives. The CXO achieves this objective through consistent branding materials that easily convey DIR messaging and value and this branding has been embraced agencywide. Since the CXO's inception (previously called the Program Development Office) in 2019, the Office has completed over 1,000 design and publication projects in support of the agency.

DIR's most externally facing asset is the DIR website, which DIR redesigned in 2021 to better promote what DIR does, and why it matters. The CXO is also the content owner of the DIR website and oversees the Website Content Governance Team. In 2022, the DIR website had the following statistics:

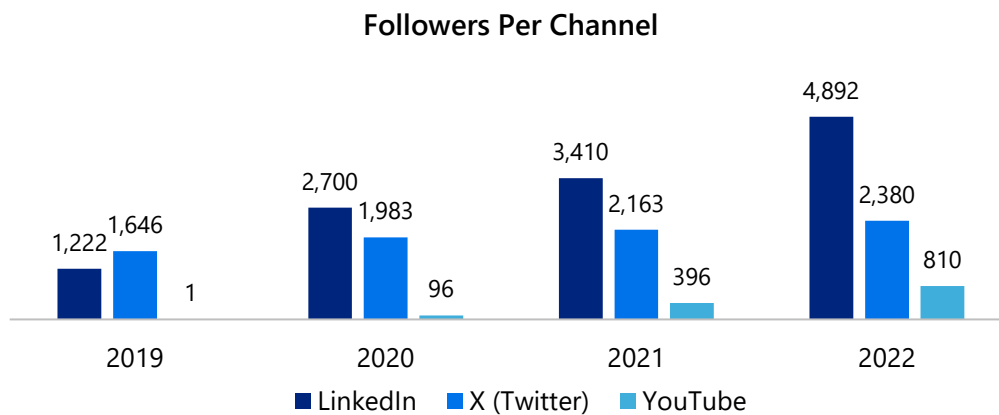
- A 0.35 percent bounce rate (average bounce rate for most sites: 25 percent).
- Indicates visitors are not leaving the website or "bouncing" back to previous page after viewing only one page.

¹⁵³ [Gov't Code Chapter 552](#).

- Average time on page: 1:25 minutes (industry average is 1:12 minutes).
 - Indicates that the user finds the content interesting or engaging enough to spend time on it.
- Pages per session: 1.83 minutes (average is two minutes).
 - Indicates that the average visitor is interested in exploring the website beyond the initial page they land on. Also, a good indication that visitors find what they are looking for without having to click through too many pages.

Under the Chief Experience Officer's direction, DIR's social media following increased 64 percent between 2021 and 2022 across all DIR channels and platforms (LinkedIn, Twitter, YouTube), including 88k views on DIR's YouTube channel, more than any previous year.

Figure 8 Followers per Channel



Chief Financial Office

The Chief Financial Office has managed the agency's growth from a \$261 million budget in 2013 to a \$467 million budget in 2023, all while maintaining approximately 30 current full-time employees. Through the Chief Financial Office's Shared Services Financial Analysis and Telecom Accounts Receivable and Payable departments, the Chief Financial Office assists with managing approximately \$557.6 million (in fiscal year 2022) in services consumed by DIR customers by negotiating financial terms and prices, performing contract management and monitoring functions specific to financial terms and conditions, and disputing vendor charges where necessary. These activities effectively provide the financial management of these contracts and vendors so that DIR's customers can focus more on mission critical information technology implementation and operations.

While the growth in the agency's budget is certainly one way to gauge the impact of the Chief Financial Office, other indicators of the support that this division provides to DIR, its customers, and other stakeholders include:

- Providing financial oversight for the Texas.gov portal, which processed approximately 57.4 million transactions totaling \$2.3 billion in revenues for Texas government entities in 2022;
- Ensuring DIR's collection of all fees due from Cooperative Contracts sales. Total sales and administrative fees increased from \$1.8 billion and \$7.4 million, respectively, in 2013 to \$3 billion and \$21.2 million, respectively, in 2022;
- Successfully disputing \$7.3 million in telecommunications charges and \$2.5 million in shared technology services charges in 2022;
- Providing financial oversight for ten Shared Technology Services contracts, which delivered a combined total of approximately \$407 million in services to customers in 2022;
- Assisting state agency customers with the Shared Technology Services portion of their Legislative Appropriations Requests;
- Serving as a resource to Legislative Budget Board staff as it considers customer agencies' budget requests; and
- Supporting agency growth in headcount from 196 employees in 2013 to approximately 250 current full-time employees in 2023.

Information Security Officer

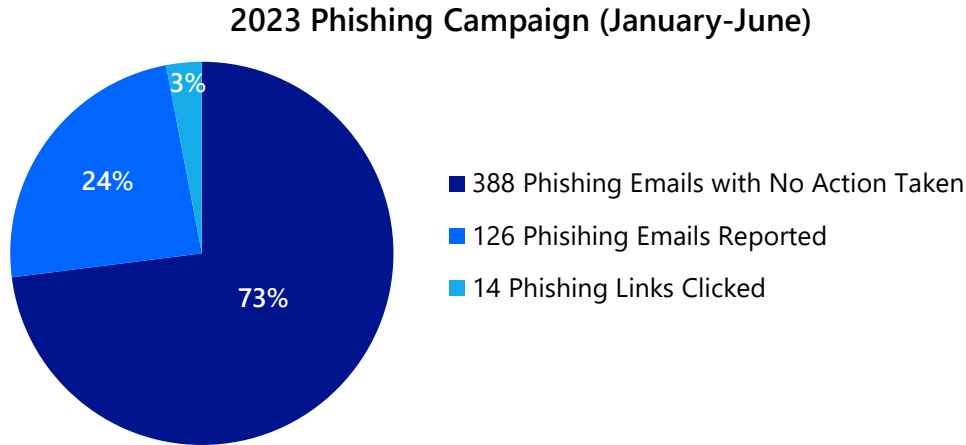
The DIR ISO administers the Texas Cybersecurity Framework assessment for DIR. The Texas Cybersecurity Framework is intended to help an organization better understand, manage, and reduce its cybersecurity risks. In March 2022, the ISO assessed DIR against the Texas Cybersecurity Framework, finding that DIR achieved an overall maturity score above the state average.

The ISO ensures compliance with [Government Code Section 2054.5191](#), which requires certain state employees to complete certified cybersecurity training. In 2022 and 2023, DIR achieved 100 percent compliance with this requirement.¹⁵⁴

The ISO conducts phishing exercises quarterly, which involve simulating phishing emails sent to DIR employees to test their ability to identify and report such threats. Each quarter, the number of DIR employees who reported phishing emails increased while the number of phishing links clicked by DIR employees decreased. The chart below shows the combined results for the first two quarters of 2023 (January through June.)

¹⁵⁴ [Gov't Code § 2054.5191](#).

Figure 9 2023 Phishing Campaign (January-June)



Information Technology Services Team

The Information Technology Services (ITS) team is responsible for the technology facets of DIR's website, which went through a major upgrade in 2020 to improve user experience and content management. DIR also moved the website to the public cloud to provide additional scalability and leverage improved search engine and system support. The DIR website comprises nearly 600 individual pages that provides access to over 2,700 active and inactive contracts, as well as information on 7,800 vendors with active and inactive DIR contracts, and over 1,200 downloaded resource documents.

The ITS team helps DIR staff with technology issues through a ticketing process. DIR staff report an issue through an online form, and the issue is then assigned to an ITS staff member for resolution. The help desk team is discussed in more detail in Section (f), but, in fiscal year (FY) 2022, six full-time employees and two contractors resolved more than 4,100 help tickets from DIR's employees who were spread across three buildings, as detailed in the chart below.

Figure 10 IT Support Tickets by Area FY22

IT Support Area	FY22 Tickets
IT Applications	2,270
IT Services	596
Microsoft Applications	445
Website Support	314
Hardware/Software Procurement	278
Permission	158
Password Reset	61
Loan Item	18
Unlock Network Account	11
ADA Compliance Accessibility	5
Total	4,156

Chief Compliance and Risk Officer

The Compliance and Risk Officer is a regular participant in most executive management discussions, helping ensure that high standards of customer service, market responsiveness, and innovation are balanced with a consideration for the risks to taxpayer funds, Texans' data, and uncompromising compliance with legal restrictions at all times.

The Compliance and Risk Officer assists all areas of DIR in analyzing problems, generating insights for better decision-making, and maintaining a holistic view of DIR's risk portfolio. The Compliance and Risk Officer regularly engages in efforts to operationalize streamlined compliance strategies at all levels of DIR management, create or revise business process documentation, and help create a more compliance and risk-aware culture among DIR employees.

The Compliance and Risk Officer oversaw the creation and launch of a Knowledge Management team at DIR, which is managing the comprehensive overhaul and refresh of DIR's documentation for internal policies, charters, and standard operating procedures. This team will ultimately provide both a framework for ensuring such documentation stays current and facilitate the input of institutional memory and best practices into DIR's learning management program. These efforts are the first steps toward creating a truly comprehensive enterprise risk management program for DIR.

In addition, the Compliance and Risk Officer has accomplished the following since the role's creation in 2019:

- Helped review and reposition a compliance strategy for the Payment Card Industry Data Security Standards within the Texas.gov program;
- Assisted in the establishment of a new statewide technology center that facilitates adoption of new technologies, especially cloud-driven applications and software products;
- Completed a comprehensive review of DIR's approval processes;
- Completed a master signature authority matrix for the entire agency;
- Served as a single point of contact with executive-level decision authority during DIR's Risk Management Program Review performed by the State Office of Risk Management;
- Monitored both internal and external audits of DIR, advised management on audit findings, and helped develop solutions that remediated the risks identified in such findings; and
- Worked closely with DIR's Internal Audit division to provide a comprehensive understanding of DIR's risk portfolio so that DIR's management is fully conversant with the annual audit plan and the insights gained through internal audits.

People and Culture Office

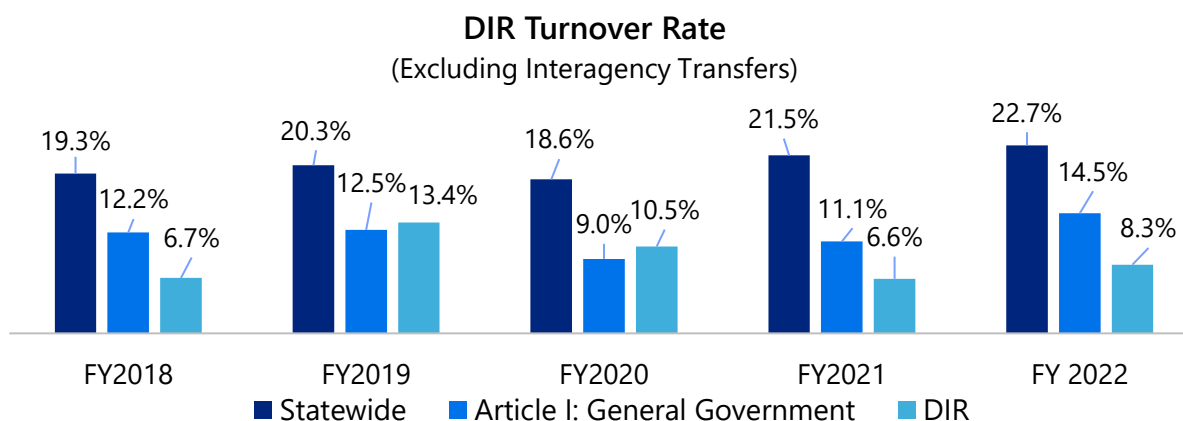
The People and Culture Office oversees and administers DIR's employee engagement program. Through this team's efforts, DIR received its highest employee engagement rating since the

agency began participating in the Survey of Employee Engagement, which measures employee experience and workplace satisfaction in compliance with [Government Code Section 2056.0021](#). In 2023, 75 percent of DIR's workforce was engaged or highly engaged in the agency whereas nationwide survey results reflected only 30 percent of employees fell into this category. Employee engagement is a critical metric that evaluates employee programs developed and managed by the People and Culture Office.

The People and Culture Office also creates and oversees programs that improve employee retention and decrease employee turnover. Through these programs, DIR counted a 14.3 percent turnover rate in FY22, far below the state's total turnover rate of 24.5 percent, according to the State Auditor's Office.

The chart below shows DIR's turnover rate against other agencies in Article 1 of the General Appropriations Act (GAA), and against the state as a whole for FY18-22.

Figure 11 DIR Turnover Rate



The People and Culture Office influences and shapes DIR's culture through the development and adoption of programs that reinforce its core values and rewards employee success through innovative recognition programs. In 2021, 2022, and 2023, DIR has received Top Workplaces awards among employers with 150-499 employees in Austin and nationwide, based on employee feedback given through an anonymous third-party survey. This designation is based solely on employee feedback to an anonymous survey administered by Energage, LLC. The survey measures 15 "culture drivers" that Energage deems "critical to the success of any organization." DIR's employees ranked the agency against well-known organizations in both the private and public sectors.

Workplace safety is managed by the People and Culture Office. The Worker's Compensation Coordinator and Safety Officer reside within this Office, working jointly to reduce workplace injuries and incidents through employee education and awareness. Under this Office's leadership, DIR's workforce has not experienced an employee injury in more than three years.

Project Management Office

The Project Management Office tracks each DIR project according to the schedule and cost

performance as related to variances from an agreed upon baseline.

During the planning phase, the Project Management Office estimates a project schedule with agreement from the project team and sponsor. The Project Management Office determines a baseline for the project schedule and captures it in the project portfolio management system. If the Project Management Office determines that the project will not be completed within the baselined duration, this will be reflected as a schedule variance that is calculated and captured in DIR's project portfolio management system.

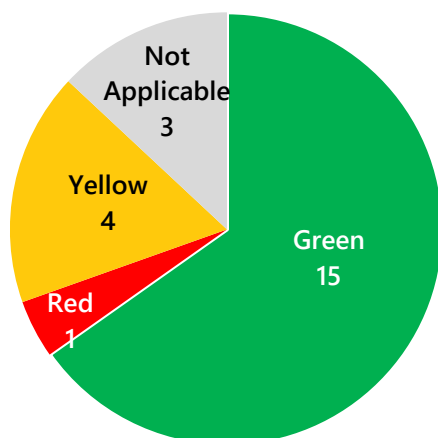
For each project, the Project Management Office assigns a Red/Yellow/Green "health indicator" to each project based on schedule and cost performance metrics shown below.

Figure 12 Red/Yellow/Green Health Indicator Metrics

	Red	Total Schedule Variance or Budget Variance > 25% (difference between baseline and planned schedule) and/or project issue with high threat level, impacting schedule, scope, and/or budget.
	Yellow	Total Schedule Variance or Budget Variance = 15% to 25% (difference between baseline and planned schedule) and/or project issue or risk, potentially impacting schedule, scope, and/or budget.
	Green	Total Schedule Variance < 15 % (difference between baseline and planned schedule) and/or project issues with low threat level, impacting schedule, scope, and/or budget, but not beyond acceptable variances of 15%.

The following chart shows the status of DIR projects assigned a Project Manager from the Project Management Office in July 2023.

Figure 13 DIR Projects Assigned a Project Manager in July 2023



Office of Public Affairs and Strategic Initiatives

The Office of Public Affairs and Strategic Initiatives is dedicated to educating the state's leadership on DIR's mission and provided services. In the past several years, the Office worked to increase DIR's visibility and strengthen the agency's relationships with the Legislature and

the Office of the Governor. The Office of Public Affairs and Strategic Initiatives participates in weekly state agency communication calls with the Governor's press office, meets regularly with the Governor's policy liaison, and communicates immediately on urgent matters. Since 2019, the agency has been successful in gaining legislative approval for multiple cybersecurity projects and initiatives to improve the cybersecurity posture of state and local government entities, including the creation of the Regional Security Operations Center, the Volunteer Incident Response Team, and the Texas Risk and Authorization Management Program. Also, during that time, the Office of Public Affairs and Strategic Initiatives worked with the Legislature to create the Statewide Chief Data Officer and State Chief Information Security Officer, who both, among other duties, help provide guidance to other government entities in their respective subject matter areas. Detailed information on DIR's recommendations regarding statutory changes is in Section VIII. Statutory Authority and Recent Legislation.

The Office of Public Affairs and Strategic Initiatives maintains DIR's legislative tracking webpage, which provides information about technology, cybersecurity, and contracting legislation, and regularly presents legislative updates to inform DIR customers, vendors, and other stakeholders on pending bills and the implementation of new statutes.

In the 87th Legislative Session, the Office of Public Affairs and Strategic Initiatives tracked 328 bills relating to technology, cybersecurity, contracting, Texas.gov, and other agency matters. During that session, the Legislature passed—and the Governor subsequently signed—all of the agency's recommended statutory changes that directly impacted the agency. The Office of Public Affairs and Strategic Initiatives worked closely with state appropriators and DIR was appropriated over \$40 million in new funding through the General Appropriation Act and all supplemental bills for cybersecurity initiatives to help state and local government entities. This funding included approximately \$22 million for endpoint detection and response (EDR) technologies for state agencies and higher education, approximately \$13.8 million for the implementation of Senate Bill 475, including funding for a pilot Regional Security Operations Center, and \$4 million for additional multifactor authentication services for state agencies and higher education.

In the 88th Legislative Session, public affairs tracked 294 bills relating to technology, cybersecurity, contracting, Texas.gov, and other agency matters. During that session, the Legislature passed—and the Governor subsequently signed—80 percent of the agency's recommended statutory changes that directly impacted the agency. The Office of Public Affairs and Strategic Initiatives again interacted with state appropriators to ensure understanding of DIR's roles and funding requests. As a result, DIR maintained the cybersecurity funding for state and local government entities appropriated in the 87th Legislative Session and received approximately \$24.5 million more for the next two years. The Legislature also appropriated \$11 million to DIR for two new Regional Security Operations Centers, \$2 million for increased cybersecurity logs capacity on the DIR-run state network, and \$4.6 million in new Texas.gov security initiatives. In addition to funds appropriated directly to DIR for cybersecurity, the Legislature created an interagency cybersecurity initiative, which provided \$55 million to the Texas Education Agency to improve cybersecurity at K-12 schools through an interagency agreement with DIR. Additionally, the Legislature recognized the growth of DIR's workload and

increased DIR's full-time equivalent (FTE) employee count from 228 to 267, an increase of 17 percent, to help the agency with the additional responsibilities and increased customer utilization of DIR's services. The Legislature also granted DIR authority to fund a new e-Procurement system, and a new Vendor Sales Reporting System to improve procurement functions.

d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

Office of General Counsel

2022

In 2022, DIR established the position of Privacy Officer within the Office of General Counsel. The Privacy Officer ensures that the agency prioritizes the consideration of privacy matters and how DIR uses and protects Texans' personal information in all technology projects and initiatives. As privacy laws are currently evolving at a rapid pace, having an agency resource with extensive knowledge on privacy laws, relevant privacy certifications, and the ability to advise on the laws' applicability to current and developing projects is a necessity.

Chief Experience Office

2019

In 2019, the Executive Director established the Program Development Office to better streamline outreach and communication efforts to ensure agency alignment with DIR's vision of transforming Texas government and its statutory mandate to provide security, solutions, and services to all levels of Texas government. The Program Development Office was tasked with:

- Coordinating DIR program outreach and development activities with holistic, unified, and consistent branding and messaging;
- Developing and implementing growth strategies for current programs; and
- Managing DIR's digital presence, social media, campaigns, and events, including the design and content of DIR's website.

2020

In 2020, the Program Development Office redesigned the DIR brand, which included the development of brand guidance, templates, and approved content for general agency use; the goal of these changes was to provide consistent messaging and a cohesive look and feel across the agency as well as to external stakeholders. The Program Development Office created DIR's brand as "the trusted guide" for statewide technology, expressing this brand through templates and guides for all DIR programs and services.

2022

Customer service is the one product that all government should deliver to its constituents. It is

at the heart of what government is intended to do. Accordingly, in October 2022, the Program Development Office introduced the customer experience initiative for DIR with the ultimate goal of being intentional in how DIR interacts with our customers to create ideal customer experiences across DIR programs. While exceptional customer experience has been a pillar of DIR's strategic vision since 2020, the Program Development Office formalized it as a function of the Office with the announcement of the customer experience initiative. The Program Development Office facilitates collaboration with and guides divisions through the customer experience maturity model while also managing the newly established customer experience focus group. Through this focus group, representatives from every DIR division can provide input to the overall customer strategy, assist in determining customer needs, and inform customer journeys and process improvements. As DIR programs continue to advance and evolve to meet the fast-changing technology landscape, PDO ensures DIR customers are aware of and can implement these solutions to support their organizations' mission and goals.

2023

In 2023, the Executive Director transitioned the Program Development Office to the Chief Experience Office (CXO) to lead and mature the agency's customer experience strategy. The Chief Experience Office is tasked with:

- Establishing, developing, and managing the agency's customer experience program and strategies;
- Coordinating DIR program outreach and development activities with holistic, unified, and consistent branding and messaging;
- Developing and implementing growth strategies for current programs; and
- Managing DIR's digital presence, social media, outreach campaigns, and events, including the design and content of DIR's website.

Risk and Compliance Officer

2019

Texas law¹⁵⁵ requires DIR's Board to employ an Internal Auditor who reports directly to the board and to provide the auditor with the resources necessary to support their role. In furtherance of this directive, DIR's executive management is committed to providing Internal Audit with resources to help maximize the benefit of the Internal Auditor employed by DIR's Board of Directors and preserving the independence and access of the Internal Auditor without interference; DIR's leadership, however, also highly values the advice and assistance of the Internal Auditor in making strategic and operational decisions for the agency.¹⁵⁶

In 2019, in recognition of the importance of the Internal Auditor's role, DIR created the Risk and Compliance Officer position in executive leadership to increase compliance and risk

¹⁵⁵ [Gov't Code § 2054.038\(a\).](#)

¹⁵⁶ [Gov't Code § 2054.038\(d\).](#)

management efficiency, which furnished the Internal Auditor with a direct point of contact with senior level authority and objectives inherently aligned with those of Internal Audit. Doing so helps ensure that other leaders comply with auditor requests in a timely and comprehensive manner, that remediation efforts based on audit findings are properly managed, and that management considers and acts on risks or compliance deficiencies identified by the Internal Auditor.

People and Culture Office

In the past, DIR followed a traditional human resources (HR) model where the Human Resources Office dedicated most of their time to administrative and transactional duties such as:

- Processing forms;
- Administering basic HR functions such as benefits, time, and leave;
- Performing traditional compensation duties;
- Implementing ideas from the agency's leadership team;
- Supporting disciplinary actions (often after the issues escalated into risks and legal concerns); and
- Traditional recruiting duties, including posting jobs, sending resumes to managers, and processing hiring trends.

Prior to its designation as the People and Culture Office, the Human Resources Office was not viewed as a strategic partner in agency decision-making, and it reacted to workforce trends rather than proactively preparing for change.

2020

In 2020, DIR announced the transition of its Human Resources Office role to the People and Culture Office, which provided a more holistic and modern approach to the agency workforce than the previous human resources functions did.

2023

In August 2023, DIR announced the appointment of the Chief People and Culture Officer to executive management, ensuring that the important initiatives that this Office supports had an executive advocate with an in-depth knowledge of the programs and projects.

Today, the People and Culture Office is a modern institution focused on DIR's people, culture, and long-term sustainability. While still performing the traditional administrative HR functions, the People and Culture Office also:

- Creates and implements strategies to attract, recruit, hire, and retain top talent by evaluating projected future developments and long-term agency plans and objectives;
- Hosting intake meetings with hiring managers;
- Sourcing and screening applicants;
- Providing input on hiring decisions;
- Administering assessments;
- Conducting compensation studies to ensure DIR's workforce is paid equitably;¹⁵⁷ and
- Providing salary recommendations.

Transitioning from a traditional human resources model to a people and culture model has boosted agency morale, improved turnover, enhanced retention rates, increased employee satisfaction ratings, provided local and national recognition, and created a thriving workforce environment.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

Generally, there are no qualifications or eligibility requirements that the Agency Administration function impacts, although the division mostly interacts with entities that are eligible for DIR's

¹⁵⁷ Equitable pay is provided to maintain salary equality between or among agency employees or in comparison to employees in similar positions in relevant job markets. Texas Comptroller of Public Accounts, [Salary Adjustments for State Agency Employees](https://fmxcpa.texas.gov/fm/pubs/paypol/general_provisions2/index.php?section=salary_adjust&page=salary_adjust#top), https://fmxcpa.texas.gov/fm/pubs/paypol/general_provisions2/index.php?section=salary_adjust&page=salary_adjust#top.

services. The programs under the Agency Administration function affect employees of DIR and assist in the operation and communication of DIR programs for eligible entities.

f) Describe how your program or function is administered, including a description of the processes involved in the program or function.

Administration

Executive Director/Deputy Executive Director

The Executive Director is responsible for administering the functions of the agency and reports directly to DIR's Board of Directors. The Deputy Executive Director reports to the Executive Director.

DIR consolidated external relations, outreach, planning, policy, reporting, digital accessibility, data management, and customer experience activities within the Deputy Executive Director's Office. The Deputy Executive Director currently oversees the following departments: Compliance and Risk Management Office; Chief Experience Office; Project Management Office, the Office of Public Affairs and Strategic Initiatives, the Office of Chief Data Officer as mentioned in the Data Management function, and Customer Engagement Office referenced in the Shared Technology Services and Texas.gov function sections.

Through those Offices, the Deputy Executive Director has oversight over many cross-functional activities including the outreach, training, data analysis, and reporting activities mentioned in the IT Procurement and Contracting function, and activities for planning, policy, reporting, digital accessibility, and IRM outreach and education activities mentioned in the Technology Guidance and Innovation function.

The Executive Director and Deputy Executive Director lead the agency's Executive Leadership Team (ELT), which currently meets four mornings a week to discuss agency matters. ELT consists of the Executive Director, the Deputy Executive Director, the Chief People and Culture Officer, the Chief Operations Officer, the Chief Information Security Officer, the Chief Procurement Officer, the Chief Technology Officer, the Chief Financial Officer, the Chief Risk Officer, the Chief Experience Officer, and the Director of Public Affairs and Strategic Initiatives.

Office of General Counsel

The Office of General Counsel currently has seven Attorney positions (including one General Counsel role and six Assistant General Counsel roles) and one Legal Assistant position.

The General Counsel role reports to the Executive Director and is responsible both for managing Office of General Counsel team members and providing executive legal decisions regarding DIR's programs and responsibilities. This individual is also the escalation point for legal issues the agency encounters.

One of the Assistant General Counsels serves as the Privacy Officer. This role:

- Provides legal advice, guidance, and training on privacy matters;

- Reviews all DIR contracts and procurements involving personally identifiable information to ensure the protection of constituent data by vendors and third parties;
- Coordinates with the ISO to establish an internal incident response plan;
- Assists other agencies with incident response when a data breach occurs;
- Ensures agency policies and procedures comply with state and federal privacy laws and best practices; and
- Participates in DIR's artificial intelligence (AI) initiatives to ensure that privacy principles are considered as the state looks to incorporate AI into its business operations.

Three Assistant General Counsels, as well as the newly added Attorney position, are responsible for providing legal counsel and support on:

- Procurements and contracts in DIR's Cooperative Contracts program;
- Internal DIR purchases;
- Procurements for Shared Technology Services procurements; and
- Legal advice and counsel regarding all Shared Technology Services programs.

One Assistant General Counsel is responsible for all administrative law functions, including employment and labor issues, rule and policymaking, public information, and records management.

The Office of General Counsel houses the Ethics Office. The General Counsel role is DIR's Chief Ethics Officer, who acts as the escalation point for all ethics issues impacting DIR. All Assistant General Counsels are Ethics Officers for DIR and are responsible for providing ethical guidance to the DIR Board and employees.

All Assistant General Counsels may be tasked with general legal research and analysis as required or necessary for a DIR program.

Chief Experience Office

The Chief Experience Office consists of eight employees: Chief Experience Officer, Outreach and Customer Experience Manager, Brand and Customer Experience Manager, Digital Community Coordinator, the Statewide Digital Accessibility Administrator, the IRM Outreach and Education Manager, the IT Procurement and Contracting Outreach and Training Coordinator, and a Cybersecurity Outreach and Education Coordinator. All employees of the Chief Experience Office collaborate with all DIR divisions on customer experiences.

The Chief Experience Officer oversees the Chief Experience Office and is a member of executive management, reporting to the Deputy Executive Director. The Chief Experience Officer primarily focuses on customer engagement and external engagements.

The Outreach and Customer Experience Manager supports the Customer Advisory Committee required by statute in addition to developing and implementing customer surveys and newsletters for coordinated outreach. This individual also serves as the DIR Website Content

Manager and oversees the DIR Website Content Governance Council. This individual manages the customer experience initiative through developing the program vision and materials, educating DIR employees, consulting with divisions, and facilitating agency strategies.

The Brand and Customer Experience Manager is responsible for the brand experience of the agency, which includes the design of agency materials and consulting with DIR staff on agency publications. This individual manages the customer experience initiative through developing the program vision and materials, educating DIR employees, consulting with divisions, and facilitating agency strategies.

The Digital Community Coordinator leads all digital content and social media for DIR.

The Outreach and Training Coordinator is further discussed in VII. Guide to Agency Programs - IT Procurement and Contracting.

The Statewide Digital Accessibility Program Administrator and IRM Outreach and Education Manager are further discussed in VII. Guide to Agency Programs - Technology Guidance and Innovation.

The Cybersecurity Outreach and Education Coordinator is further discussed in VII. Guide to Agency Programs - Cybersecurity.

Chief Financial Office

The Chief Financial Office is led by the Chief Financial Officer and is composed of 30 FTEs. This Office includes the following teams:

- Budget and Finance;
- Accounting; and
- Shared Services Financial Analysis.
- **The Budget and Finance team** is led by a Budget Director, who manages three Budget Analysts. The Budget and Finance team's main functions include establishing and maintaining appropriate budget controls for the agency to ensure compliance with the General Appropriations Act and other related statutes and rules, consulting with agency departments and management to develop the biennial legislative appropriations requests and annual operating budgets and working with legislative oversight agencies such as the Legislative Budget Board.
- **The Accounting team** is responsible for general ledger accounting, accounts receivable, accounts payable, payroll processing, and financial reporting. Reports emphasize generally accepted accounting principles and include deliverables required by the Texas Comptroller of Public Accounts. The Director of Accounting oversees 18 full-time employees across four functional areas:
 - **General Ledger Accounting and Accounts Receivable**, which is composed of one Manager and six Accountants who are responsible for general ledger accounting, financial reporting, and accounts receivable;

- **Accounts Payable and Travel**, which is composed of two accountants who are responsible for processing payments to external suppliers and coordinating travel plans and reimbursing employees for travel expenses incurred while conducting agency business;
- **Payroll** which is administered by one payroll officer; and
- **Telecom Accounts Receivable and Accounts Payable**, which is composed of one Manager and seven Accountants who are responsible for ensuring that Texas Agency Network (TEX-AN) vendors correctly bill for services consumed by DIR customers and, when necessary, dispute charges.
- **The Shared Services Financial Analysis Team** performs all financial activities for DIR's Shared Technology Services. This team is led by a Director, who oversees five Budget Analysts that are responsible for the following:
 - Participating in contract negotiations, specifically regarding financial terms and conditions, evaluating vendor prices for services;
 - Managing financial issues associated with DIR's Shared Technology Services and telecommunications contracts and vendors;
 - Helping state agencies prepare their Legislative Appropriations Requests with regards to their use of DIR's Shared Technology Services;
 - Assisting the Legislative Budget Board with its oversight of agencies' appropriations requests related to Shared Technology Services;
 - Proposing DIR fee changes to executive management and to the DIR Board of Directors;
 - Overseeing Shared Technology Services monthly invoicing activities, performing vendor financial stability checks for DIR contracts; and
 - Assisting with onboarding new Texas.gov payment processing customers.

Information Security Officer

The Information Security Officer reports to the Chief Technology Officer with the following responsibilities:

- **Developing and Maintaining Security Plans and Policies:** The ISO is responsible for creating an agency-wide information security plan as required by law.¹⁵⁸ The ISO also recommends, develops, and maintains security policies and procedures that address the agency's specific security risks.
- **Working with Business and Technical Resources:** The ISO collaborates with other divisions within the agency to ensure that all internal security requirements are met by implementing mandatory controls to address the agency's information security risks.¹⁵⁹
- **Training and Direction:** The ISO provides training and guidance to staff who have

¹⁵⁸ [Gov't Code § 2054.133](#).

¹⁵⁹ The mandatory controls are listed in the [DIR Security Controls Standards Catalog](#).

significant responsibilities for information security, which ensures that all staff understand their responsibilities and can effectively contribute to the agency's security efforts. Texas law mandates each state agency identify state employees who use a computer for at least 25 percent of the employee's required duties to complete a cybersecurity training certified by DIR.¹⁶⁰

- **Guidance and Assistance:** The ISO provides guidance to senior agency officials, information owners, information custodians, and end users about their responsibilities under the agency's security policies.
- **Risk and Security Assessments:** The ISO ensures that risk assessments and security assessments are conducted regularly. These assessments help identify potential vulnerabilities and ensure that the agency's security measures are effective.
- **Reviewing Information Systems Inventory:** The ISO reviews the agency's inventory of information systems and determines who is responsible for each system.
- **Policy Recommendations:** The ISO recommends agencywide policies, procedures, and practices to ensure the security of the DIR's information and resources, often collaborating with DIR's Information Resources Manager, information owners, and custodians to develop and implement these policies.
- **Coordinating Security Requirements Review:** Before acquiring new information systems or services, the ISO coordinates a review of the security requirements and verifies that there are risk mitigation plans in place.
- **Reporting on the Security Program:** The ISO reports to the Executive Director at least annually on the status and effectiveness of the security program.
- **Non-compliance:** If DIR is non-compliant with its security policies, the ISO must inform the relevant parties.
- **Issuing Exceptions:** With the approval of the Executive Director, the ISO may issue exceptions to DIR information security requirements or controls. These exceptions must be justified, documented, and communicated to the appropriate parties.

Information Technology Services Team

The Information Technology Services (ITS) team ensures the availability and effectiveness of the agency's operational systems. The ITS team works to build and enhance the effectiveness and efficiency of the systems leveraged across DIR, provides technical project services for IT systems projects, and works with DIR business leaders to prioritize the efforts and resources necessary to support these projects.

The ITS team also provides support for the technological needs of DIR's executive management, agency employees, contractors, and DIR Board members. These technological needs encompass the team's management of DIR's internal business systems and computing infrastructure.

The ITS team is under the Chief Technology Office and includes four functions:

¹⁶⁰ [Gov't Code § 2054.519](#).

- Business analysis;
- Compliance and improvement coordination;
- IT application delivery; and
- IT operations.

The Director of ITS is designated as DIR's Information Resources Manager (IRM).¹⁶¹

The team includes approximately 19 current full-time employees and two contractors who report to a management team of three (IRM, Operations Manager, and Applications Manager).

Business Analysis

The Business Analysis function improves the quality of ITS, analyzes business needs, and team members serve as liaisons for the IT department when working with other program areas to identify and coordinate the automation of new or improved systems while enhancing business operations.

The IT Business Analyst oversees this area and is responsible for ensuring operational compliance through key information technology services, providing training, access, and support for internal and external projects through the code repository tool that DIR uses to conduct QAT (Quality Assurance Testing) and UAT (User Acceptance Testing). This role also assists in guiding divisions in improving processes, products, services, and software through ITS operations governance.

Compliance and Improvement Coordination

The Compliance and Improvement Coordinator provides high level internal coordination, planning, and management services for the ITS management team. The role collaborates with agency stakeholders and the Project Management Office to lead strategic projects and continuous improvement projects leveraging ITS resources, a process that often includes defining strategies, outlining milestones, and coordinating and tracking tasks to completion. Generally, this role monitors and mitigates project risks and promotes best practices for project execution. Their specific responsibilities include:

- Engaging vendors and contractors;
- Acting as the Project Manager for ITS projects;
- Overseeing change management;
- Providing audit support; and
- Developing ITS processes and procedures.

IT Operations

The IT Operations team includes the IT Operations Manager, a senior-level Systems Administrator, two Database Administrators, two Program Systems Analysts, a System Support

¹⁶¹ [Gov't Code § 2054.071](#).

Specialist, two Help Desk System Analysts, and two help desk contractors. The team supports the agency desktop environment by:

- Installing, maintaining, and troubleshooting endpoint software, hardware, and file/print/fax services;
- Performing systems management and integration; and
- Resolving IT-related issues for DIR employees, customers, vendors, and contractors.

The team manages the technical infrastructure necessary to support internal applications and systems including servers, databases, and related technologies in addition to acting as the primary technical resource that support agency telecommunications fulfillment and billing services.

The responsibilities of IT Operations include:

- Tracking inventory and software compliance;
- Providing the primary support for the agency's help desk for technical issues;
- Overseeing the agency's account management; and
- Providing email support, and hardware and software configuration.

The team also provides server support and system administration, network design, and planning for the Shared Technology Services, including the Data Center Services (DCS) program.

IT Application Delivery

The IT Application Delivery team provides development and support for applications available externally and internally to DIR. This team provides IT support for the implementation of new systems through project management, system analysis design, and programming. The IT Application Delivery team includes three Developers providing support for over 50 applications and data repositories such as the DIR website and six public application portals for customers and vendors.

DIR has integrated application delivery services across all aspects of the agency with DIR's IT Application Delivery team continually aiming to improve ease of information access, provide secure data exchanges, and increase the cost effectiveness of application delivery solutions.

Internal Audit

Internal Audit consists of one Internal Audit Manager,¹⁶² who reports directly to the DIR Board of Directors. Due to persistent and long-term recruitment and retention challenges within the

¹⁶² This is the functional title for the appointed Internal Auditor that the DIR Board is required to employ pursuant to Government Code § 2054.038.

Internal Audit division, explained in detail in Section (m) below, DIR's Board,¹⁶³ in conjunction with DIR's Executive Director, restructured the Internal Audit function as a managed outsourced model. Under this model, DIR outsources the majority of its audit work to qualified private-sector audit firms while retaining an Internal Auditor, acting in their role as Internal Audit Manager, who oversees those firms and reports directly to the DIR board on all Internal Audit functions. Given the workforce challenges that DIR faces, restructuring was the only option to mitigate the substantial risk of not having the robust and efficient audit function that DIR requires to ensure compliant, efficient, and effective operations.

DIR's Internal Audit Manager provides strategic direction for all Internal Audit functions and serves as the Project Manager for any and all audits performed by external audit firms. The Internal Audit Manager conducts an agencywide risk assessment and annual audit plan, prepares DIR's annual audit report, and coordinates with external audit firms to ensure completion of the audits listed in the annual audit plan. Execution of such duties includes:

- Providing program information;
- Approving audit scope and deliverables;
- Coordinating and scheduling meetings with DIR staff;
- Ensuring program areas respond to information requests;
- Tracking key milestones; and
- Approving final audit reports.

In addition, the Internal Audit Manager verifies that changes made in response to audit findings or recommendations are completed and documented and consults on programmatic compliance and risk management strategies.

The Internal Audit Manager also works directly with the State Auditor's Office to submit required reports and conduct follow-up activities on recommendations outlined in State Auditor's Office audit reports.

The Internal Audit Manager serves as the Project Manager for planned audits by providing project information, identifying agency resources, scheduling interviews, tracking, and submitting information requests, and working with DIR management to ensure that responses are submitted as required.

The Internal Audit Manager is statutorily tasked with completing an annual audit plan, which guides the overall operation of the Internal Audit function by using risk assessment techniques to rank high-risk functions at DIR.¹⁶⁴ This process begins in late spring or early summer of each

¹⁶³ DIR's Audit, Finance, and Legal Subcommittee evaluated the resources available to the Internal Audit division as authorized by Government Code § 2054.040(b) and determined the appropriate sufficient resources. On October 27, 2022, DIR's Board approved a motion relating to the appointment of an Internal Auditor in an open meeting.

¹⁶⁴ [Gov't Code § 2054.038\(b\)](#).

year. To prepare the risk assessment, the Internal Audit Manager first interviews DIR's executive management about obstacles that could prevent the agency from reaching its strategic goals, generally starting with a discussion of risks identified during the prior year's risk assessment, before proceeding to interview program or function level managers to discuss the same questions.

Based on this input, the Internal Audit Manager then creates a risk table outlining potential risks to the agency and their impact, based both prior risks and those identified through the interview process, and assigns a rating to each identified risk based on the likelihood of the risk event occurring and the severity of harm DIR would experience should it occur. The Internal Audit Manager creates the proposed annual audit plan based upon the outline that they generate during the process. Upon completion of the annual risk assessment and audit plan, the Internal Audit Manager presents the findings and proposed plan to relevant DIR Board subcommittees before presenting the proposed audit plan for approval by the DIR Board at a scheduled open meeting.

After the DIR Board approves the annual audit plan, the Internal Audit Manager uses their independent judgment to determine the order in which Internal Audit will pursue planned audits, considering audit resources and the business operations of DIR. Internal Audit works with relevant Chief Procurement Office and Office of General Counsel employees to craft statements of work that adequately describe the scope and nature of audit activities that need to be undertaken. Internal Audit circulates the completed statements of work among the audit firms DIR has under contract, which allows firms to respond with proposed audit plans, pricing, and related materials. Based on these materials, DIR selects a firm to perform the requested audits based upon the evaluation criteria established by DIR to determine the best value to the state.

Once DIR awards a statement of work, the Internal Audit Manager serves as the point of contact for the contracted audit provider and independently manages and oversees the audit activities performed by the audit firm and supports the Chief Procurement Office's management of the awarded contract. To accomplish this role, the Internal Audit Manager:

- Holds entrance conferences and status check-ins;
- Answers questions and coordinates document requests as required by the audit provider; and
- Reviews and accepts all deliverables created by the contracted audit provider as part of the audit.

In FY23, the Internal Audit Manager created a Request for Qualifications (RFQ) to solicit and obtain master contracts with audit firms that will be used to perform audits contained in the annual audit plan. DIR awarded contracts to six qualified applicants to provide audit services. The Internal Audit division created Statements of Work (SOWs) for the audits identified by the annual audit plan, responded to respondent questions, and served as an evaluator for solicitation responses.

With the assistance of the audit contractors under the new audit structure, the Internal Audit

Manager completed three outstanding audits from the FY22 audit plan. These audits would not have been completed using the previous department structure.

The Chief Compliance and Risk Officer

The Risk Management function is fulfilled by the Chief Compliance and Risk Officer and the Compliance and Training Coordinator.¹⁶⁵ By designating the Chief Compliance and Risk Officer as the sole person responsible for enterprise risk management at the agency, DIR promotes consistency and continuity in how risk management advice is given to management. The Compliance and Training Coordinator ensures the completion of diverse tasks without taking the Chief Compliance and Risk Officer's focus from agencywide compliance strategies and initiatives.

With oversight from the Chief Compliance and Risk Officer, the Compliance and Training Coordinator leads the DIR Knowledge Management Team, which sets consistent expectations for drafting, updating, and reviewing documentation of internal business processes. The Knowledge Management Team is a cross-disciplinary team made up of the Chief Compliance and Risk Officer, the Compliance and Training Coordinator, Knowledge Management Team ambassadors, and advisors from the Office of General Counsel, Internal Audit, and other select areas of the agency. Knowledge Management Team ambassadors volunteer from DIR's various business areas and aid designated business areas of the agency as they develop, draft, and update business process documentation within their area.

The Chief Compliance and Risk Officer and Compliance and Training Coordinator perform administrative oversight responsibilities, including:

- Identifying documentation needs;
- Guiding and facilitating document creation and updates;
- Performing and coordinating document review with organizational units;
- Maintaining the documentation storage repository referred to as the knowledge management system; and
- Tracking when documents are due for review.

People and Culture Office

The People and Culture Office is focused on the agency's workforce, culture, long-term sustainability, and digital transformation of people and culture practices using data driven decision-making techniques such as workforce trend forecasting and salary comparisons. The People and Culture Office is a valuable partner to DIR's leadership, with the Chief People and Culture Officer advocating for people and culture initiatives as a member of DIR's executive management, and the People and Culture Office as a whole supporting senior leaders, managers, and supervisors in strategy execution, the delivery of administrative efficiencies, serving as a champion for employees, and acting as an agent of continuous transformation to

¹⁶⁵ The compliance and training coordinator is also a part of DIR's People and Culture Office.

shape processes and a culture that improves DIR's capacity for change.

The People and Culture Office is led by the Chief People and Culture Officer, who supervises the agency's Human Resources (HR) functions and leads the vision, strategy, development, and execution of talent and culture management programs to advance the agency's mission, vision, and core value statements. The Chief People and Culture Officer:

- Develops policies and procedures;
- Advises on all issues related to DIR's talent, culture, and engagement;
- Administers and monitors the effectiveness of people programs;
- Works with the Office of the General Counsel and the Chief Compliance and Risk Officer on the agency's efforts to comply with federal, state, and local employment laws; and
- Supports agency management and staff in the areas of workforce planning, learning and development, performance management, employee engagement, talent management, total rewards, wellness, compliance, and culture.

Six employees report, in whole or in part, to the Chief People and Culture Officer, including one People and Culture Lead, one Training and Compliance Coordinator who is shared with the Compliance and Risk Office, three People and Culture Specialists, and one Property Manager.

The People and Culture Lead is responsible for:

- Championing positive employee experiences;
- Serving as a trusted advisor in fostering a culture of respect and appreciation; and
- Proactively collaborating with agency managers to implement talent strategies and executing people practices.

The People and Culture Lead also develops and interprets policies and procedures to further the mission, vision, and core values of the agency, implements initiatives, and ensures DIR's compliance with federal and state laws and regulations.

The Training and Compliance Coordinator role is shared with the Compliance and Risk Office. The Training and Compliance Coordinator is responsible for identifying, leading, and implementing a wide variety of agencywide continuous improvement initiatives to enhance effectiveness and compliance, including developing, documenting, implementing, and tracking the agency's standard operating procedures, policies, and training programs in compliance with all applicable state, federal, and agency-related requirements.

Two of the three People and Culture Specialists are responsible for administering people and culture programs, performing HR practices and people operations, including recruitment and selection, onboarding and offboarding, compensation, classification, employee relations, employee recognition, time and leave, and benefits administration, and ensuring compliance with state and federal laws and regulations.

One of the three People and Culture Specialists also serves as the agency's receptionist, who is the primary point of contact for agency calls and inquiries from customers. This individual also

administers and assists in HR program administration, including recruitment and selection, compensation, classification, employee relations, and leave and benefits.

The Property Manager oversees DIR's vehicle fleet and coordinates property operations, maintenance, administrative functions, and technical support. The Property Manager is also DIR's Safety Officer; in this role, they assist in the coordination of the agency's safety program by ensuring compliance with risk management factors.

Project Management Office

The Project Management Office is responsible for developing and maintaining a project management methodology for DIR. The Project Management Office is part of the Chief Operations Office and is under DIR's Deputy Executive Director. Its responsibilities include:

- Providing project management services on projects including project scope development and management, schedule development and monitoring, budget and cost development and monitoring, risk and issue management, documentation management, communications, and lessons learned and continuous improvement;
- Assisting agency leadership by prioritizing the agency's project portfolio management;
- Managing and facilitating the initiation of projects; and
- Sequencing projects based on available resources.

The Project Management Office is composed of four staff: the Project Management Office Director and three Project Managers. The Project Management Office Director administers the Project Management Office and oversees three Project Managers. The Project Management Office Director is also accountable for maintaining DIR's project management methodology, delegating project management assignments, and working with executive leadership to prioritize and manage the agency's project portfolio.

The three Project Managers contribute to the maintenance and continuous improvement of the agency's project management methodology, provide project management services on projects assigned by the Project Management Office Director, and provide DIR employees with additional assistance beyond the role of a traditional Project Manager, such as assisting the Office of Public Affairs and Strategic Initiatives in tracking legislation during legislative sessions, as necessary.

Office of Public Affairs and Strategic Initiatives

The Office of Public Affairs and Strategic Initiatives includes five current full-time employees: the Director of Public Affairs and Strategic Initiatives; the Director of Media and Government Relations; the Director of Planning, Policy, and Reporting; a Policy Analyst; and a Technical Writer.

The Director of Public Affairs and Strategic Initiatives is a member of DIR's executive leadership team and reports to the Deputy Executive Director. This role is responsible for all aspects of the Office of Public Affairs and Strategic Initiatives duties with a key focus on agency legislative

priorities and budget matters including overseeing the creation and submission of all fiscal notes related to the agency, interactions with the Legislature, and guidance and oversight provisions to other divisions on legislative and budget matters.

The Director of Media and Government Relations reports to the Director of Public Affairs and Strategic Initiatives. This role is responsible for the agency's legislative agenda during legislative session, including tracking and monitoring all legislation, assisting the Director of Public Affairs with priority legislative items, responding to media inquiries, and drafting agency press releases, talking points, and other external communications. The Technical Writer reports to the Director of Media and Government Relations.

Both the Director of Public Affairs and Strategic Initiatives and the Director of Government Relations provide guidance to other agencies and divisions on implementation of information technology legislation

The Director of Planning, Policy, and Reporting reports to the Director of Public Affairs and Strategic Initiatives and the role is further discussed in the Technology Guidance and Innovation Function. The Policy Analyst reports to the Director of Planning, Policy, and Reporting.

Agency Administration Processes

Office of General Counsel

The Office of General Counsel (OGC) handles the processes of onboarding and training new DIR board members, responding to public information requests submitted to DIR, and conducting rule reviews and amendments.

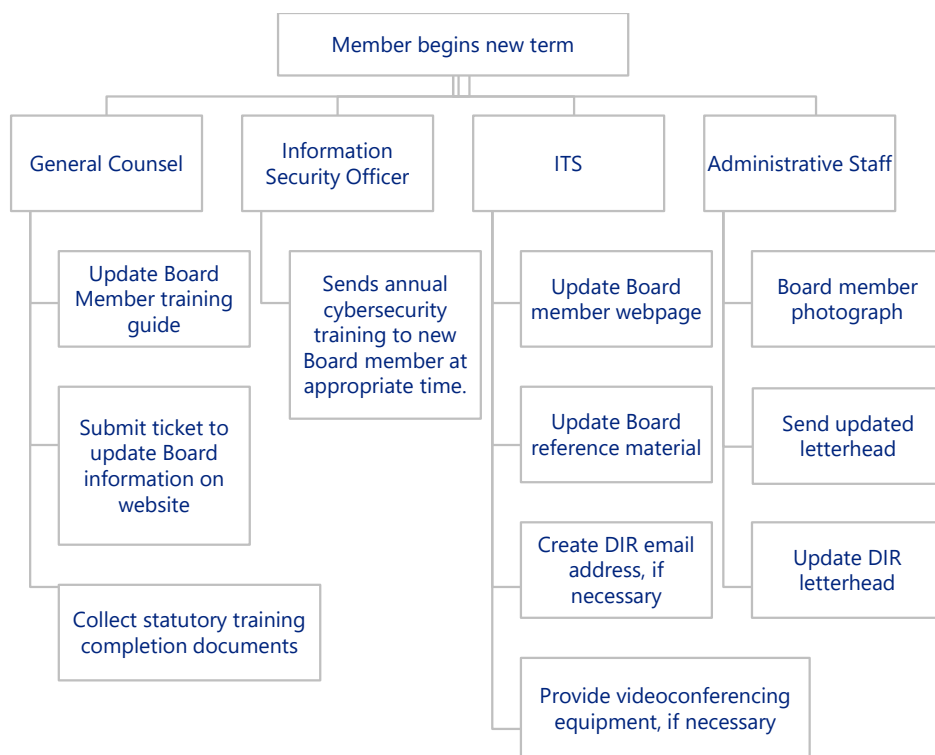
Board Onboard Process

When a DIR Board member is onboarded, DIR must complete a number of tasks to fully onboard the Board members. This begins at the time of appointment by the Governor or statutory appointment.¹⁶⁶ Board members are provided with details for the various trainings they are required to take and instructions for how to access them. These trainings are described in more detail in Section IV. (f) above. OGC also advises new board members on any ethical or conflict of interest issues and is available to answer any questions about DIR or their role as a board member. Lastly, OGC tracks and records the completion by our board members of their required training and sends reminders as necessary to ensure completion.

The OGC, in collaboration with ITS, the Information Security Officer, and Administrative Staff, administers the DIR Board onboarding process. The Administrative Law Attorney oversees board training.

¹⁶⁶ [Gov't Code § 2054.021](#).

Figure 14 DIR Board Member Onboarding Process



Public Information Process

The OGC manages the process to respond to public information requests submitted to DIR in alignment with the requirements of the Texas Public Information Act.¹⁶⁷ Upon receipt of a public information request, the Public Information Officer or their designee evaluates the request to determine whether the request provides sufficient information or description to identify responsive documents; if it does not, DIR will collaborate with the requestor to clarify any aspects of the request that are unclear. Once the request is sufficiently clear to allow for identification of the requested information, the OGC will then conduct an initial determination of whether we have information responsive to the request. If DIR does not have any responsive information, the Public Information Officer or their designee will send a response to that effect to the requestor.

If OGC does not know if DIR has responsive information or is aware that there is responsive information but does not maintain the information within the OGC, the Public Information Officer or their designee will forward the request to an open records liaison in the DIR business units where that information is likely to reside. The open records liaison will then collaborate with staff in the business unit for which they are responsible for compiling all responsive information. OGC will provide guidance as questions may arise.

¹⁶⁷ [Gov't Code Chapter 552](#).

Once OGC gathers the information, the open records liaison will provide the documents to the Public Information Officer or their designee in the manner specified by those individuals and will notify them that they have provided the responsive information.

The Public Information Officer or their designee will then review the provided documents to determine if there is any information that DIR believes to be confidential that should not be disclosed publicly. If the Public Information Officer determines that the responsive information is subject to a confidentiality exception, they will brief the exception to the Office of the Attorney General and provide copies of the briefing to the requestor and any necessary third parties. Following submission of this briefing, the Public Information Officer or their designee will produce any public information that DIR does not assert is confidential under the Public Information Act and make any redactions the requestor has agreed to, or the OAG has issued a prior determination on.

Once the OAG issues its letter ruling on DIR's (or a third party's) exception briefing, DIR will comply with instructed redactions, release the redacted information and any information that the OAG has otherwise identified as non-confidential, and provide the OAG's determination to the requestor.

Rule Reviews and Amendments

The OGC manages the process of adopting new rules, conducting rule reviews in compliance with statutory requirements, and making amendments to current rules. When the Legislature passes legislation that grants new rulemaking authority to DIR, the OGC works with the relevant business units and executive administration to determine whether rulemaking is necessary to implement the new law. If so, the OGC will work with appropriate internal stakeholders to identify the needs of the rulemaking and craft rules that align both with the requirements and the objectives of the new statutes and assist in the implementation of the law. The OGC will also work with any necessary external stakeholders, such as customer agencies, local governments, vendors, trade groups, and the Information Technology Council for Higher Education, to craft rules that accomplish the needs of the statute and result in zero to minimal impact to external stakeholders.

DIR reviews its rules on a four-year basis¹⁶⁸ to ensure the continued need for the rules and their overall efficacy. DIR may also review specific rules on an as needed basis as laws and technologies change. If DIR is opening a rule for review, then the OGC will publish the notice of rule review to the *Texas Register*, signifying that the review has begun. The OGC will not submit a notice of rule review if the amendment takes place outside of the four-year rule review cycle.

The OGC will work with the impacted business units to review the current rule and determine whether there is a continued need for the rule and, if so, whether it should be amended to address changes in law, technology, or other matters. If amendments are required, the OGC will

¹⁶⁸ [Gov't Code § 2001.039](#).

develop a draft of the amended rule in collaboration with the appropriate business units and, following the draft's creation, work with interested internal and external groups. At this time, the OGC will provide the proposed rule to the appropriate executive management and the Information Technology Council for Higher Education for review.

Once a proposed new rule or an amendment to an existing rule is drafted and reviewed by appropriate executive management and the Information Technology Council for Higher Education, the OGC presents the proposed rule to the DIR Board for consideration and approval to post in the Texas Register for public comment.

Once a rule has been posted for no less than 30 days, the OGC will review any public comments received during the public comment with the DIR business units and executive administration to determine whether the comment requires any changes to the proposed rule before taking the rule to the DIR Board for adoption. Once the rule package is finalized, it is then presented to the DIR Board one last time for the formal adoption of the rule. The DIR Board has the opportunity to consider the final rule, all public comments and DIR's response to them, and determine whether adoption of the proposed rule is appropriate. If the DIR Board votes to adopt the new or amended rule, the OGC will post the formal notice of the adoption in the Texas Register. If the adoption concludes the quadrennial rule review, then the OGC will also submit a notice of rule review closure to the *Texas Register*, signifying the conclusion of the rule review.

Information Security Officer

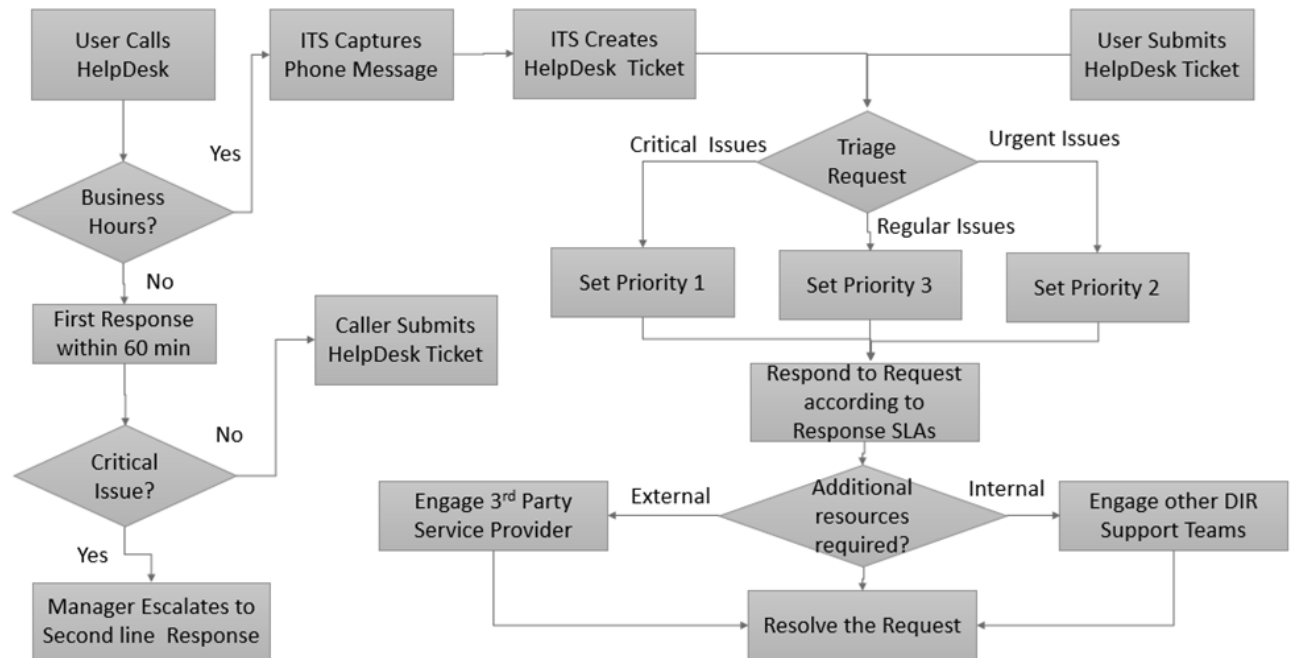
The Information Security Officer (ISO) is responsible for managing the processes associated with the continuity of operations planning. This includes a summary of the required actions to be taken to provide for the continuity of government in case of a significant event, such as a natural disaster, mechanical malfunction, or terrorist attack, that necessitates that DIR evacuate its primary facilities. The continuity of operations plan and procedures ensure that DIR can reestablish its operations and execute DIR's primary mission-essential functions, including protecting the state's IT infrastructure and supporting state agencies with IT services, in the scenario of a significant event. Processes that ensure effective implementation and management of the program include the:

- Maintenance of a succession list, which identifies key staff responsible for critical functions and establishes a clear order of succession in the event of a disaster or emergency in which the primary employees are unavailable;
- Establishing and maintaining a Memorandum of Understanding, which establishes DIR's agreement with Angelo State University and defines their respective roles, responsibilities, and mutual assistance arrangements in the event of a disaster; and
- Updating and review an essential personnel listing, which is a comprehensive compilation of staff responsible for critical functions within the agency.

Information Technology Services Team

The chart below reflects the IT Operations' ticket intake process for the help desk.

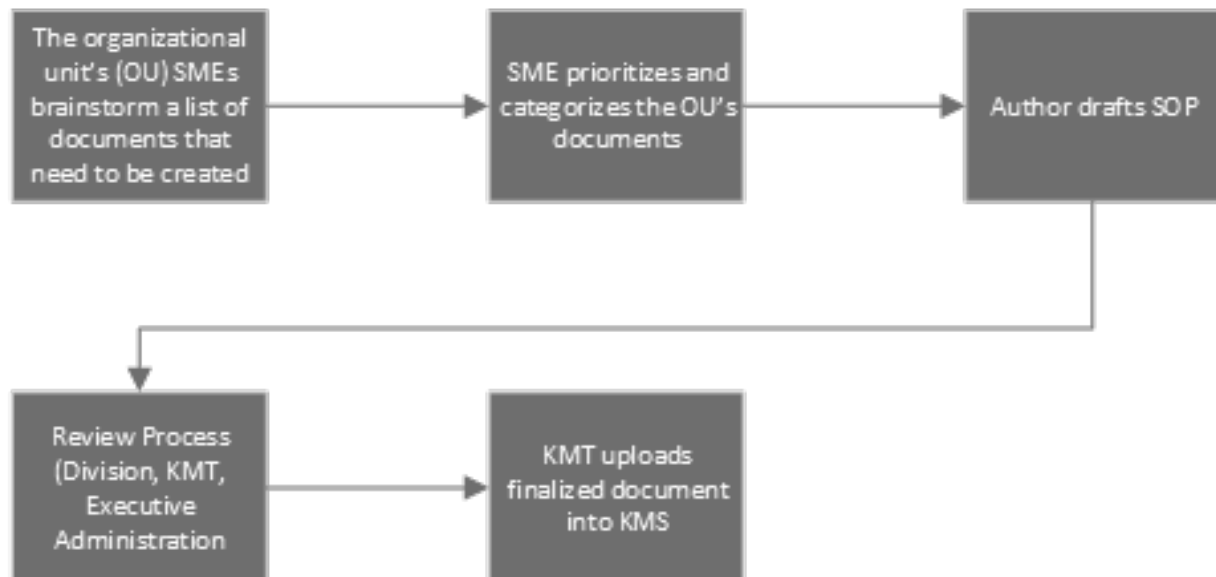
Figure 15 IT Operations' Ticket Intake Process



Risk and Compliance Officer

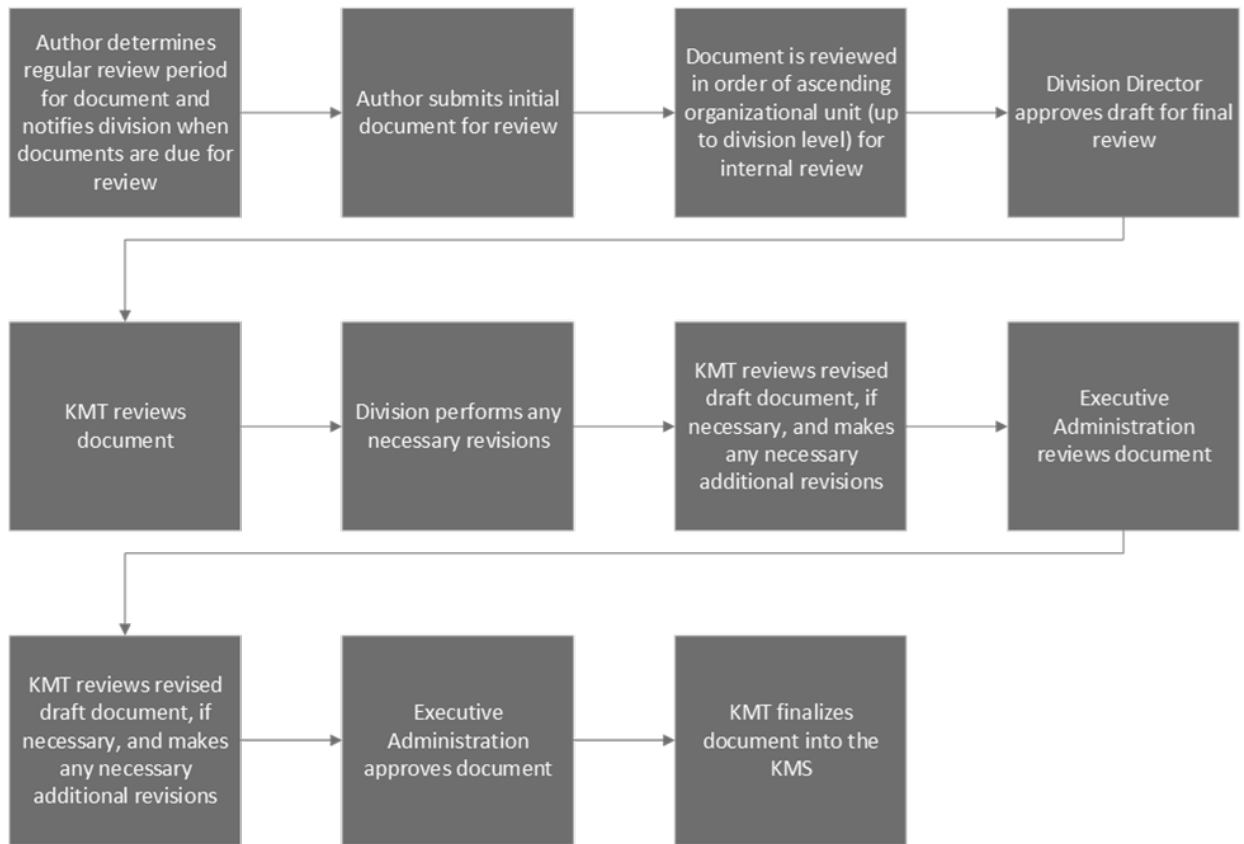
Below is the process for the initial drafting of documentation in the standard format.

Figure 16 Process for the Initial Drafting of Documentation



The following chart outlines the periodic review and updating of business process documentation on a permanent, periodically reviewed basis.

Figure 17 Periodic Review and Updating of Business Process Documentation



People and Culture Office

DIR's People and Culture Office's processes are included in DIR's employee handbook, which is provided in the attachment section.

Chief Experience Office

The CXO provides guidance and direction to DIR employees on how to communicate a consistent message to DIR's audience through the DIR Brand and Style Guide, which include links to templates and forms for requesting design and publication help from the Office. CXO has also established an eight-step sequence for DIR's Customer Experience (CX) initiative.

Figure 18 CX Components Sequence



Project Management Office

The Project Management Office's standard operating procedures document contains the Office's policies and procedures.

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

Funding for the Agency Administration function comes from multiple revenue sources as appropriated to the agency in the General Appropriations Act as discussed in Section V. Funding.

Figure 19 Method of Finance by Strategy

Strategy	Method of Finance	Amount
A.1.1 - Statewide Planning and Rules	Clearing Fund	\$87,573
A.1.2 - Innovation and Modernization	Clearing Fund	\$60,468
B.1.1 - Contract Admin.	Clearing Fund	\$1,160,671
B.2.1 – DCS	Statewide Technology Account	\$966,263
B.3.1 - Texas.gov	Statewide Network Applications Account	\$321,698
B.4.1 - Communications Technology Services	Telecommunications Revolving Account	\$2,481,333
C.1.1 - Security Policy and Awareness	Clearing Fund	\$410
C.1.2 - Security Services	Clearing Fund	\$3,494
C.1.2 - Security Services	General Revenue	\$125
D.1.1 - Central Admin.	Clearing Fund	\$675,117
D.1.1 - Central Admin.	Telecommunications Revolving Account	\$1,236,923
D.1.1 - Central Admin.	Statewide Technology Account	\$668,195
D.1.1 - Central Admin.	Statewide Network Applications Account	\$263,033
D.1.2 – IRM	Clearing Fund	\$607,329
D.1.2 – IRM	Telecommunications Revolving Account	\$1,109,855
D.1.2 – IRM	Statewide Technology Account	\$601,431
D.1.2 – IRM	Statewide Network Applications Account	\$238,074
D.1.3 - Support Services	Clearing Fund	\$120,972
D.1.3 - Support Services	Telecommunications Revolving Account	\$221,559
D.1.3 - Support Services	Statewide Technology Account	\$119,680
D.1.3 - Support Services	Statewide Network Applications Account	\$47,105

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

Not applicable.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

Not applicable.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

DIR exists to serve other public entities. State agencies, institutions of higher education, and local governments are eligible customers of the agency's programs. DIR's Agency Administration function interacts with these entities frequently and in a variety of ways, focusing on providing information and ensuring customer service. Certain Agency Administration functions, such as the Office of General Counsel and the Risk and Compliance Office, do not work with local, regional, or federal units of governments as their role is intended to provide internal guidance and council to ensure DIR's compliance with state and federal requirements.

Chief Financial Office

The Chief Financial Office bills local government entities that purchase DIR's Shared Technology Services and telecommunications services. The Office ensures that customers are billed only for the services that they consume, disputing charges that are inconsistent with the underlying vendor service contracts.

Chief Experience Office

The Chief Experience Office facilitates DIR's outreach and communication to DIR customers and eligible entities, including local and regional governments entities, by distributing monthly newsletters about DIR contracts, programs, and initiatives, sending occasional messaging on DIR time-specific initiatives, conducting IRM education and outreach activities, administering the statewide digital accessibility program, and attending various regional and local conferences across the state.

The Office also administers the DIR Customer Advisory Committee, which includes representation from all DIR customer segments, including state agencies, institutions of higher education, local governments, K-12 schools, and a member of the public.

Office of Public Affairs and Strategic Initiatives

The Office of Public Affairs and Strategic Initiatives serves as a liaison between DIR and other government entities, including municipalities, K-12 schools, counties, special districts, other state agencies, statewide elected officials, and U.S. Senate and Congressional offices. The Office of Public Affairs and Strategic Initiatives responds to requests from these entities regarding agency programs, agency activities, legislative information, and other inquiries.

k) If contracted expenditures are made through this program, please provide:

A Short Summary of The General Purpose of Those Contracts Overall

The contracts in this program are primarily used for information technology goods and services, audit services, and other professional services.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$5.2 million in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 181 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from September 2021 through August 2022 for these contracts. The funding sources for these contracts include revenues from the Cooperative Contracts, communications and technology services, Texas.gov, and shared technology services programs.

The Method Used to Procure Those Contracts

The method used to procure these contracts includes open market, invitation for bids, and direct award.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-TPC-MSA-432	Atos Governmental IT Outsourcing Services, LLC	Provides data center consolidation services for DIR's information technology applications.	\$1,024,232.84
DIR-CPO-4549	4 Consulting Inc.	Provides staff augmentation services for DIR.	\$792,746.45
DIR-TSO-4288	Carahsoft Technology Corporation	Cooperative contract that provides software, Software-as-a-Service products, and related services.	\$465,603.73
DIR-PCM-MSA-436	Rackspace US, Inc.	Provides public cloud services to DIR through the shared technology services program.	\$456,334.00
DIR-TSO-4007/SOW-09-FY21-SA-0016	The North Highland Company LLC	Provides procurement assistance for telecommunications and shared technology services.	\$380,000.00

The Methods Used to Ensure Accountability for Funding and Performance

Program and Contract Managers are responsible for ensuring that goods and services are delivered in accordance with contracts.

A Short Description of Any Current Contracting Problems.

Not applicable.

l) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

Attracting, hiring, and retaining top talent in the Austin Metroplex is challenging, particularly for the technology sector. These barriers to talent acquisition are most apparent when DIR is trying to fill information technology, cybersecurity, and technology procurement positions. DIR is competing in the same talent pool as private sector companies, which have expanded budgets, increased perks, and higher total compensation offerings. In addition, DIR loses talent to larger agencies who have multi-layered tiers for career growth, higher FTE staffing counts, and turnover savings that provide flexibility for salary budgets and increased job offers.

Internal Audit

Like many state agencies, DIR's Internal Audit function has been plagued by staffing challenges. Since 2009, DIR has employed three internal audit executives: one from 2009 through 2014; one from 2014 through 2018; and one from 2019 through 2022. Of these Internal Audit Directors, one retired from DIR and two resigned.

During that same period, DIR employed 10 other auditors to support the Internal Audit Director. Of these, only one auditor is still employed at DIR. Two auditors transferred to another state agency, one auditor was terminated, and the remaining six auditors voluntarily separated from the agency for various reasons. DIR has retained these auditors for an average of approximately 19 months, with the median retention sitting at approximately 15 months. In general, 40 percent of auditors hired by DIR left the agency after less than one year and 70 percent have left within two years. DIR has not been able to retain any auditor longer than approximately four years.

The Internal Audit division's turnover is unique to that division and is not observed across DIR. In FY22, DIR counted only a 14.3 percent turnover rate, far below the state's total turnover rate of 24.5 percent.¹⁶⁹

DIR's difficulty in staffing the Internal Audit division has persisted, despite expending significant time and effort on recruitment and retention efforts. Since 2009, DIR has posted open positions in its Internal Audit Division 21 times. The posted positions have ranged in qualifications from the baseline of Auditor I for individual contributor roles and Auditor VI to Director IV for management roles. On 10 occasions, DIR closed such postings without extending an offer of employment due to a lack of qualified applicants. In cases where DIR successfully hired a qualified applicant, the average time from posting the position to the applicant's start date has been approximately three months.

Figure 20 Auditors on Staff

Auditors on Staff				
FY2019	FY2020	FY2021	FY2022	FY2023
1	2	3	2	1

DIR has experienced a particular challenge in maintaining staffing levels in DIR's Internal Audit division since 2019. Despite having three full-time employees allocated for this division, it has only been fully staffed once for a 16-month period from April 13, 2020, to August 31, 2021. At one time since then, DIR had two auditors on staff for approximately 30 months from November 2019 to May 2022. However, at all other times since 2019, DIR has had only one auditor, despite posting seven openings during that time.

¹⁶⁹ "Classified Employee Turnover for Fiscal Year 2022." State Auditor's Office, <https://sao.texas.gov/Reports/Main/23-703.pdf>.

As discussed above, consistent recruitment and retention challenges around the Internal Audit Division induced the DIR Board, acting through DIR's Audit, Finance, and Legal Board Subcommittee and pursuant to the subcommittee's discussions with DIR's Executive Director, to restructure the Internal Audit Division as a managed outsourced model to ensure that the Internal Auditor had sufficient resources necessary and available to perform their duties.

Under this model, DIR has an Internal Audit Manager who:

- Prepares DIR's annual audit plan, using risk assessment techniques to rank high-risk functions in the department, and presents it to the Board for approval;
- Directs and oversees the work of qualified professional audit firms to conduct audits according to the approved audit plan; and
- Works directly with DIR's management and board to conduct, report, and mediate findings of such audits.

Given the workforce challenges described throughout this section, restructuring was the only option to mitigate the substantial risk of not having a robust and efficient audit function.

At present, DIR has six highly qualified and professional outside audit firms under contracts overseen and managed solely by the Internal Auditor. These firms provide DIR with access to a workforce of fully qualified auditors who conduct all audits according to industry standards governed by all relevant audit controls. Through these contracts, DIR has access to a workforce with the capacity to conduct robust, professional audits far in excess of that available to DIR even if it was able to fully staff its internal audit department.

DIR has also dedicated an additional employee in executive management to support and complement the work of this internal audit model. In the Chief Compliance and Risk Officer's day-to-day work, they identify, remediate, and prevent the same type of compliance issues and other agency risks that dominate the attention of Internal Auditors. In furtherance of their efforts on these types of compliance issues, the Chief Compliance and Risk Officer also works closely with the Internal Audit Manager to identify and manage risks and ensures the Internal Audit Manager has the resources and cooperation of executive management needed to perform the Internal Audit function.

In addition, the Chief Compliance and Risk Officer:

- Assists in creating the annual risk assessment and audit plan under the leadership and direction of the Internal Audit Manager;
- Monitors remediation of past audit findings alongside the Internal Audit Manager; and
- Provides the Internal Audit Manager with direct knowledge of senior leadership's decision-making processes.

Because the Chief Compliance and Risk Officer is accountable to executive leadership for the same basic business functions as the Internal Audit Manager performs for the Board, the position serves to bolster the Internal Audit function at all levels.

- n) Provide any additional information needed to gain a preliminary understanding of the program or function.

Not applicable.

- o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility). For each regulatory program, if applicable, describe:

Not applicable.

- p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Communications Technology Services



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and **offering innovative and cost-effective solutions for all levels of government.**

- a) Provide the following information at the beginning of each program description.

Name of Program or Function: Communications Technology Services

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Dale Richardson, Chief Operating Officer

Statutory Citation for Program:

[Government Code Chapter 2054, Subchapter H, Telecommunications Planning](#)

[Government Code Chapter 2059, Texas Computer Network Security System](#)

[Government Code Chapter 2170, Telecommunications Services](#)

- b) What is the objective of this program or function? Describe the major activities performed under this program.

Exceptional
Total Experience



Value Through
Technology



The objective of the Communications Technology Services (CTS) function is to provide a secure statewide network for data, voice, video, and internet services for use by public entities throughout Texas, including state leadership, state agencies, institutions of higher education, and local government.

The major activities that fulfil the Communications Technology Services function are classified

under: Network Operations, the Texas Agency Network, the Capitol Complex Telephone System, and Customer Support Services.

Network Operations

DIR designed Texas' network telecommunications infrastructure to align with customer requirements for data, voice, video, and internet services, making sure to prioritize delivery of secure, high-quality telecommunications services and support to state agencies, institutions of higher education, and local government entities.

DIR provides internet services to Texas state agencies, which are required to utilize or obtain a waiver to be excluded from using DIR's provided internet services. DIR ensures that its provided internet services are scalable, secure, and constantly monitored. State agencies also receive access to the State of Texas' Data Centers in Austin and San Angelo through DIR's connectivity services.

To ensure uninterrupted connectivity and service for DIR's customers, DIR monitors network performance, implements and maintains network devices, configures routers and switches, and troubleshoots network issues to ensure uninterrupted connectivity for CTS customers. In furtherance of this effort, DIR also oversees and supports the local fiber optic network utilized to connect and transport data for customers that use DIR's cabling services.

Texas Agency Network (TEX-AN)

The Communications Technology Services function supports the Texas Agency Network (TEX-AN), which provides competitively negotiated contracts for local and long-distance voice services, wireless services, data services, internet services, Voice over Internet Protocol (VoIP) services, and other services necessary to support customers' telecommunications infrastructure.

State agencies are statutorily required to use TEX-AN for telecommunications services, though other public entities may also use the TEX-AN contracts.¹⁷⁰ In fact, the TEX-AN program is popular with voluntary customers, such as independent school districts and local governments, who take advantage of DIR's consistent, cost-effective telecommunications solutions.

TEX-AN contracts provide customers with competitive pricing; a multi-vendor environment; a broader service portfolio; service-level agreements for each vendor and service, including remediation of service issues; operational-level agreements for each vendor and each service; and availability of developing and emerging technologies.

A key activity of the TEX-AN program is to negotiate and secure competitively priced contracts with multiple vendors to allow agencies and other government entities the opportunity to obtain critical services for operating their businesses without having to negotiate multiple

¹⁷⁰ [Gov't Code § 2170.051\(c\)](#).

contracts individually.

In April 2022, DIR successfully executed new TEX-AN contracts when the previous contracts ended after their designated 10-year term. The new contracts significantly increased the number of TEX-AN vendors available to customers from five to 23, providing greater purchasing options and a range of broadband selections for state agencies and other entities.

Capitol Complex Telephone System

DIR operates the Capitol Complex Telephone System (CCTS), a centrally managed telephone service for 93 Austin area state agencies including each house of the Legislature and the legislative agencies within the Capitol Complex. DIR is responsible for providing this service under [Government Code Chapter 2170](#).¹⁷¹

Key activities include servicing more than 14,000 desk phones, soft phones, and conference phones, and managing the day-to-day operations of the system across the Capitol Complex. Management of the day-to-day operations of the CCTS includes coordinating office phone moves, additions of phone lines, and any changes necessary to accommodate an agency's preparations for legislative sessions.

Customer Support Services

To ensure service efficiency and customer satisfaction, DIR provides customer support services to assist customers from state agencies, institutions of higher education, and local governments, including placing service orders, addressing service inquiries, and resolving concerns or complaints related to data, voice, video, and internet connectivity. DIR provides project management for the state-wide communications network infrastructure, telephony management of remote state office buildings (currently El Paso, Ft Worth, and Houston), and migration of the 14,000 legacy phones on the Capitol Complex to DIR's state-of-the-art VoIP platform. DIR staff manage the video conferencing productions for DIR Board meetings, consult and manage the network infrastructure reroutes, including all fiber optic cabling moves to accommodate the Capitol Mall project, and provide consultative support to agencies and municipalities for new and emerging technologies relative to DIR offerings.

Depending on the services ordered, vendors may bill customers directly. For some services, DIR itself provides customers a single, consolidated monthly invoice of all voice, data, long distance usage, toll-free usage, CCTS charges, and DIR network services charges. These charges are payable via an online portal, which allows customers to streamline their payment of bills, rather than requiring them to manage several bills from a variety of vendors and services. DIR also reviews customer consolidated bills and disputes erroneous charges with the vendors on behalf of customers. As a result, DIR's customers do not have to expend significant resources to review their telecom charges and avoid paying incorrect charges. In 2022, DIR disputed approximately

¹⁷¹ [Gov't Code Chapter 2170](#).

\$7.3 million in telecommunications charges on behalf of customers.

Key activities include managing and processing customer voice and data circuit orders with TEX-AN's vendors, monitoring and overseeing vendor change management activities, assisting DIR's Contract Management team in vendor performance reviews for the TEX-AN contracts, overseeing vendor marketing performance management for the TEX-AN contract, and reviewing statement of work compliance of vendor proposals to state agencies.

DIR also manages service provider invoices, produces monthly consolidated billings, and monitors work orders. These tasks allow DIR to ensure that the services provided to state agencies are both cost effective and best in service.

c) What information can you provide that shows the effectiveness and efficiency of this program or function? If applicable, reference but do not repeat any performance measures from Section II, Exhibit 2, and provide any other metrics of program effectiveness and efficiency. Also, please provide the calculation or methodology behind each statistic or performance measure.

Texas Agency Network (TEX-AN)

DIR divides billing for TEX-AN services between customers who are billed by DIR and those who are billed directly by the service provider:

DIR-Billed customers receive a bill from DIR for:

- Services including long distance, data services, and Next-Gen 911 services provided by a service provider; and
- The Capitol Complex telephone service, internet services, transport, co-location services, and Domain Name System (DNS) services provided by DIR.

Direct-Billed customers are billed directly by the service provider for local voice services, small or home office internet, wireless services, and managed telecommunication services.

The chart below reflects utilization of TEX-AN contracts by both DIR-billed customers and direct-billed customers.

Figure 21 TEX-AN Customers FY2022 by Channel and Billing

TEX-AN Customers FY2022		
Channel Type	Direct-Billed Customers	DIR-Billed Customers
Assistance Org	51	N/A
Higher Education	159	112
K-12	957	240
Local Government	1976	420
Out of State	1	
State Agencies	101	130
Total	3245	902

Capitol Complex Telephone System

In FY22, the Capitol Complex Telephone System's Technicians addressed 21,811 work orders and 408 trouble tickets and operators answered 17,343 telephone calls.

d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

2010

DIR began substantial work to innovate and transform the telecommunications system in the Capitol Complex from the CCTS PBX system to the new VoIP platform. During the initial phase of this project, DIR took the role of pilot agency to test the capabilities and effectiveness of the VoIP platform. DIR dedicated a significant amount of time to thoroughly testing the platform before rolling it out to other agencies.

2012

DIR began transitioning from a 35-year-old Private Branch Exchange (PBX) voicemail and phone system to a fully integrated Voice over Internet Protocol (VoIP) platform at the Capitol Complex. This transition brought significant network improvements, including enhanced functionality, scalability, cost savings, improved productivity and collaboration, enhanced reliability, and disaster recovery features. The implementation of the new VoIP platform marks a substantial advancement in modernizing communications infrastructure and catering to the evolving needs of the State of Texas.

DIR began migrating 10 agencies, including the Credit Union Department, Ethics Commission, Veterans Land Board, Texas General Land Office, Public Utilities Commission, and others, to the shared VoIP platform. During this migration phase, DIR realized the necessity of upgrading to a Hosted Collaboration Solution (HCS) platform to effectively support multiple agencies.

2015

DIR proceeded to upgrade the VoIP platform to an HCS multi-tenant platform, making it capable of supporting multiple agencies as they migrated from the outdated PBX system. The HCS platform is designed to concurrently serve multiple agencies with each agency having their own isolated and secure environment. This setup allows state agencies to receive customized services based on individual requirements, while DIR assumes responsibility for platform maintenance, upgrades, and ongoing support.

2020

DIR approached the Texas Legislative Council, which manages the network operations for the Texas House and Senate offices in the Texas Capitol, to begin scheduling the migration of the phones at the Texas Capitol. Since then, DIR and the Texas Legislative Council have been engaged in detailed migration planning discussions regarding the Capitol Complex phones.

Several events from 2020 - 2023 have affected the completion of this phase of the project:

- According to the Texas Legislative Council, the Texas Capitol and Capitol Extension were not ready for the VoIP migration until the Texas Legislative Council completed their Network Infrastructure Overhaul project. This project was completed in mid-2022.
- The COVID-19 pandemic in 2020 caused a profound effect on the supply chain for phones and other network equipment.
- DIR, the Texas Legislative Council, and the Texas House of Representatives and Senate mutually agreed to postpone the migration until the conclusion of the 88th Regular Legislative Session and any subsequent special sessions, ultimately postponing the migration to the beginning of 2024.

2023

As of July, 88 agencies have successfully migrated to the current HCS VoIP platform. During the transition, DIR has had to pay for maintaining both systems. Once the full implementation of the new system is complete, the state will soon see significant cost savings.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The following entities are eligible for services DIR provides, including programs within the

Communications Technology Services function:¹⁷²

- State agencies;
- Local governments;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Texas Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Texas Education Code Section 5.001;
- Private schools as defined by Texas Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Texas Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Texas Tax Code Section 152.001; and
- Government entities of another state.

Texas law requires state agencies to use DIR's consolidated telecommunications system, and other eligible entities may utilize DIR's consolidated telecommunications system services.¹⁷³ While state agencies are required to use TEX-AN, other entities may do so voluntarily.

f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.

Communications Technology Services Program Administration

Much of the CTS program resides in DIR's Chief Operations Office, which is overseen by DIR's Chief Operations Officer. The Director of Program Operations manages the following teams: Network Engineering and Cabling Services, Strategic Client Solutions, and the Capitol Complex

¹⁷² Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

¹⁷³ [Gov't Code § 2170.051](#); [Gov't Code § 2170.004](#).

Telephone System.

Within DIR's Chief Operations Office, the Service Fulfillment Manager manages the Service Fulfillment team. The team responsible for administering TEX-AN contracts is under the Chief Procurement Office and the Telecom Billing team is part of the Chief Financial Office.

Network Engineering and Cabling Services

The Assistant Director of Operations and Engineering oversees the Network Operations and Engineering team,¹⁷⁴ which includes two Managers overseeing five network engineers, three Operations Specialists, and three Cabling Services Technicians. Additionally, DIR uses managed services for TEX-AN to support the team's work.

The Network Operations and Engineering team manages day-to-day operations, monitors network performance, provisions services, and ensures network security for state agencies served by CTS. In addition, they provide customer service and support for data, voice, video, Domain Name System (DNS), and internet connectivity.

Network engineers are responsible for implementing and maintaining network devices, configuring routers and switches, and troubleshooting network issues to ensure uninterrupted connectivity for CTS customers. The Cabling Services Technicians provide support of the fiber-optic cable that connects and transports customer data and oversee cabling projects for customers that utilize DIR's cabling services. The Cabling Service Technicians manage these functions through work orders and tickets, the procedures for which are outlined in CTS Processes below.

The Cybersecurity Operations team, which is part of the Chief Operations Office and discussed in detail in VII. Guide to Agency Programs - Cybersecurity, plays a crucial role supporting the Network Operations and Engineering Team and ensuring the cybersecurity of Texas by monitoring the state's network, responding to incidents, and coordinating with other DIR teams for efficient resolution of network faults.

Strategic Client Solutions

The Strategic Client Solutions team supports communications infrastructure projects and provides related support to state agencies by providing project management for the statewide enterprise communications network infrastructure; telephony management of remote state agency office buildings (currently El Paso, Ft Worth, and Houston); management of and the video conferencing productions for DIR Board of Directors meetings; management of the migration of the 14,000 legacy phones on the Capitol Complex to DIR's state-of-the-art VoIP platform; vendor marketing performance management for the TEX-AN contract; and statement of work compliance reviews of vendor proposals to state agencies. The team also consults and manages network infrastructure reroutes, including all fiber-optic cabling to accommodate the

¹⁷⁴ Also known as Connectivity Services.

Capitol Mall project, and provides consultative support to agencies and municipalities for new and emerging technologies relative to DIR offerings.

The Strategic Client Solutions team's activities are administered by a Manager and two Project Managers.

Capitol Complex Telephone System (CCTS)

The CCTS team manages the day-to-day telephone service for the state agencies' telephone lines within the Capitol Complex, including the legacy PBX services and current VoIP services. Managing this service includes maintaining the hardware, software, and physical infrastructure of the platform as well as security updating and patching. Customers order CCTS services by submitting a work order via email that includes all critical information and data necessary for the team to carry out the scope of work identified in the order.

The CCTS program is administered by a Manager, two Supervisors, six Technicians, and four work order/directory services operators. DIR utilizes the TEX-AN telecom services contract to augment the team as necessary.

The work order/directory services operators are responsible for answering incoming calls within the Capitol Complex. The operators also attend to general calls made to DIR by directing calls to the appropriate party. They are expected to greet and interact with callers in a courteous and professional manner, answering questions, and assisting with phone calls to specific state of Texas government agency telephone numbers.

Service Fulfillment

The Service Fulfillment team assists customers from state agencies, institutions of higher education, and local governments by placing service orders, addressing service inquiries, and resolving concerns or complaints related to data, voice, video, and internet connectivity. This team is under DIR's Service Fulfillment Manager and is administered by two Quality Assurance Specialists, five Client Support Specialists, and a Program Specialist.

The Quality Assurance Specialists monitor telecom vendor change requests and maintenance activities that may impact a customer's active service while delivering personalized customer service to ensure smooth communication experiences within the secure statewide network. They also provide service level agreement management of DIR-billed TEX-AN vendors and support the contract team in the Chief Procurement Office in monitoring TEX-AN vendor performance.

The Client Support Specialists and Program Specialist are responsible for the processing and oversight of all DIR-billed orders placed with DIR vendors, including service activations, moves, additions, changes, and disconnections.

Texas Agency Network (TEX-AN)

Two Contract Managers in the Chief Procurement Office manage the TEX-AN contracts. The duties and procedures followed by DIR Contract Managers are discussed at length in VII. Guide to Agency Programs - IT Procurement and Contracting.

The Contract Managers administer the program through tracking and overseeing contract deliverables, such as monthly reports, and quarterly vendor performance meetings during which the Service Delivery, Billing, and Operations teams meet with the Contract Managers to review vendor performance. Additionally, the Contract Managers work closely with TEX-AN vendors to efficiently reduce pricing and amend the contracts as necessary to make available new technology that falls within the scope of the contract. The Contract Managers also develop educational information to share with customers, present telecom overviews to customers, and manage and oversee customer service agreements, which are contracts between DIR and discretionary customers that help support billing and operations.

On DIR's website, DIR provides information about [TEX-AN contracts](#), pricing, forms that allow customers to order services, and phone numbers to connect customers with a Client Support Specialist that will assist with their needs.

Telecom Billing

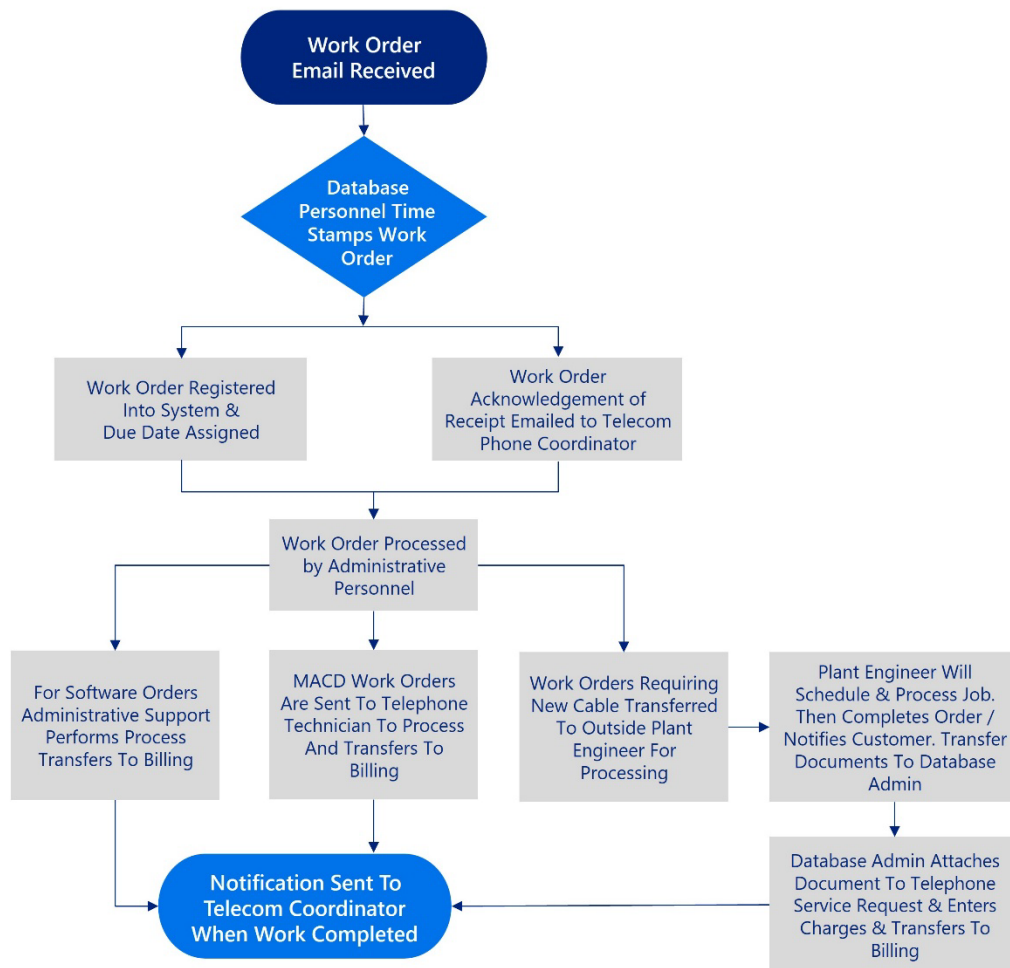
The Telecom Billing team is part of the Chief Financial Office and reports to the Director of Accounting. This team includes a Manager and seven Accountants responsible for billing customers for TEX-AN services, who ensure that customers are billed correctly for TEX-AN services by validating vendor telecom charges and disputing charges when vendors incorrectly bill customers. During 2022, DIR disputed approximately \$7.3 million in telecommunications charges on behalf of customers.

Communications Technology Services Processes

Work Order Process

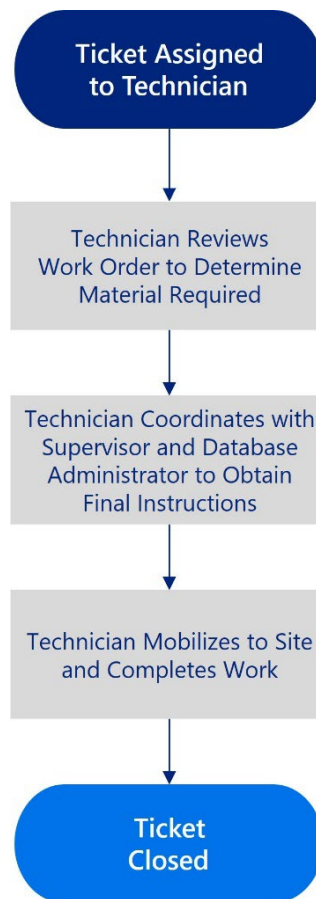
State agencies submit work orders to DIR by email to request equipment or cabling, or move, adds, changes, or deletes (MACD). This process is shown below.

Figure 22 Work Order Process



The Technician follows the process below to complete the work order.

Figure 23 Technician Process for Work Orders



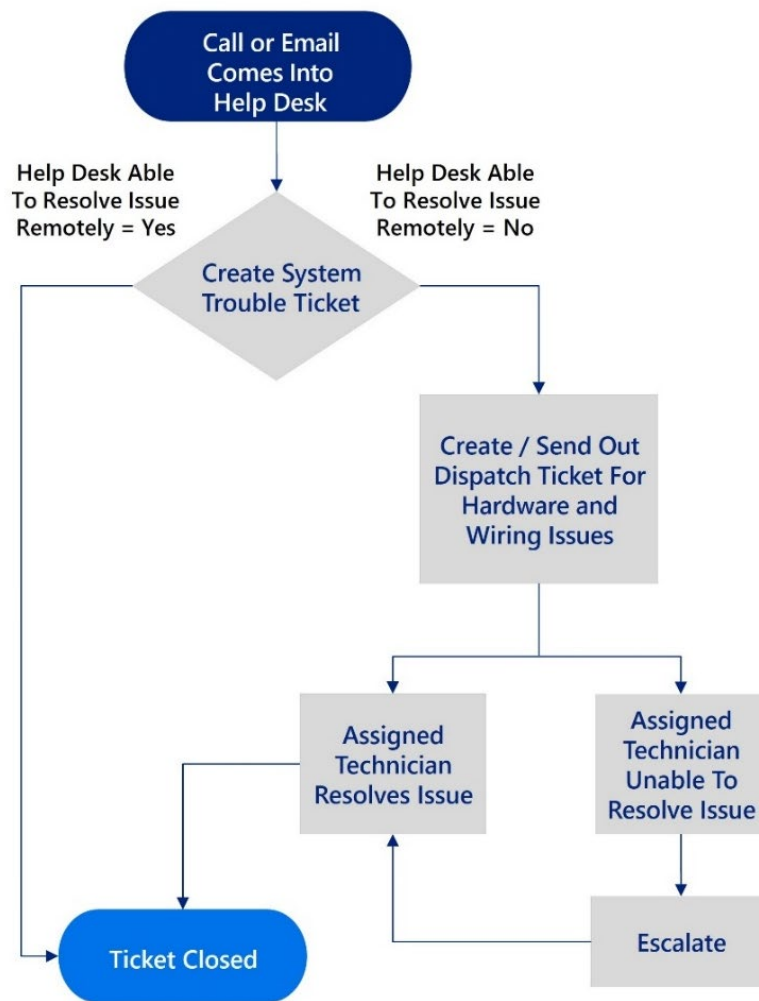
Help Desk Process

The DIR Help Desk is available for all CCTS and TEX-AN customers to request technical support.

DIR staff at the Help Desk receive emails and phone calls from customers reporting issues with DIR equipment and services. The staff who receive these communications are responsible for opening a ticket for the customer and ensuring that the customer receives timely assistance to resolve the issue as quickly as possible.

The basic Help Desk workflow steps are outlined below.

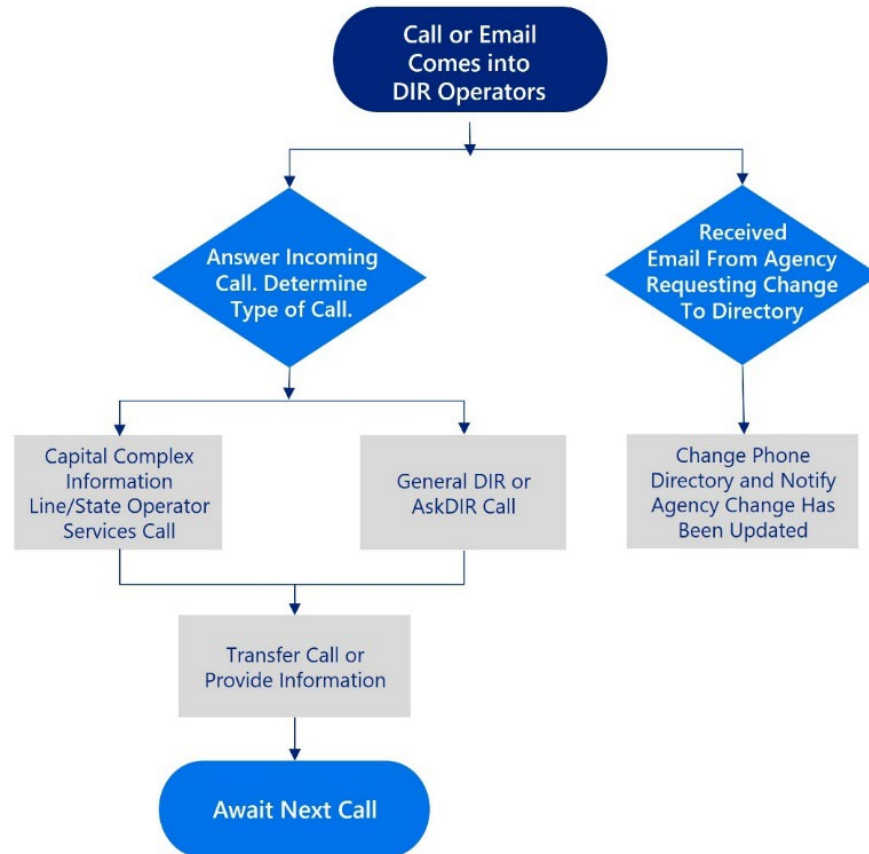
Figure 24 Help Desk Workflow



Capitol Complex Telephone System Call Operator Process

The flow chart below details the operator call intake process.

Figure 25 Operator Call Intake Process



Process for Updating the Capitol Complex Telephone System Directory

DIR maintains the Capitol Complex Telephone System Directory and relies upon agencies to provide updated information to keep it accurate. The CTS program's telecommunications specialists notify the designated state agency contact coordinators by email of the intended update and an approximate due date. This process consists of submitting a spreadsheet of the current agency contact coordinators that can be updated on a daily basis per email request.

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The Communications Technology Services function is funded by fees charged to customers for the services that they order and related to telecommunication services that entities receive from DIR. DIR bills customers for the services that they consume and deposits payments into the Telecommunications Revolving Account. These funds are then used to pay the telecommunications services providers and for DIR's operating expenses.

Strategy	Method of Finance	Amount
B.4.1 - Communications Technology Services	Telecommunications Revolving Account	\$105,071,519

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

DIR's TEX-AN program and Cooperative Contracts program do have similarities. Both TEX-AN and the Cooperative Contracts program are for purchases of automated information systems.¹⁷⁵ However, TEX-AN contracts, which are part of the Communications Technology Services function and administered by both DIR's Chief Operations Office and Chief Procurement Office, are for acquiring telecommunications services¹⁷⁶ whereas the Cooperative Contracts program, which is further discussed in VII. Guide to Agency Programs - IT Procurement and Contracting and managed by the Chief Procurement Office, is exclusively for acquiring information technology commodity items,¹⁷⁷ specifically excluding telecommunications services.¹⁷⁸ Because certain IT commodity products can be used in conjunction with telecommunications services, products available through the Cooperative Contracts program may also be available through TEX-AN. If a product of this type is available through TEX-AN, it may only be purchased when bundled with telecommunications services through TEX-AN; it cannot be purchased as a stand-alone product through TEX-AN.

DIR competitively procures both the TEX-AN and the Cooperative Contracts program so that DIR customers can compare negotiated pricing across each program's contracts. However, the Cooperative Contracts program is designed so that DIR customers always work directly with contracted vendors to obtain IT commodities available under each contract. In contrast, most purchasing under TEX-AN contracts goes through DIR with DIR providing customers with a single, consolidated monthly invoice for telecommunications services. The monthly invoice includes most services obtained through TEX-AN contracts with certain exceptions, such as wireless services, which are direct-billed through TEX-AN vendors rather than through DIR.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

DIR competitively procures contracts in its TEX-AN and Cooperative Contract programs

¹⁷⁵ [Gov't Code Chapter 2157, Subchapter A.](#)

¹⁷⁶ [Gov't Code Chapter 2170.](#)

¹⁷⁷ [Gov't Code Chapter 2157, Subchapter B.](#)

¹⁷⁸ [Gov't Code § 2157.068\(a\).](#)

through a request for offer (RFO) process. To minimize duplication and conflict, DIR's Chief Procurement Office tailors each RFO to ensure that sufficient solutions to DIR customer needs for telecommunications services (in the case of TEX-AN) and IT commodities (in the case of the Cooperative Contracts program) are available through awarded contracts. The Chief Procurement Office works closely with other DIR departments to ensure that specific technology needs for the state are addressed through the procurement process. The Chief Procurement Office reviews RFO responses to ensure that vendors are only providing products and services permitted by the RFO parameters.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

Eligible local, regional, or federal units of government of the Communications Technology Services function include:

- Local governments, including counties, municipalities, school districts, and junior college districts;¹⁷⁹
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.¹⁸⁰

DIR provides telecommunications services to local governments and school districts across the state of Texas through the TEX-AN contracts.

DIR is a part of the Greater Austin Area Telecommunications Network ([GAATN](#)), which is a joint effort of DIR, the Austin Independent School District, City of Austin, Travis County, Austin Community College, University of Texas at Austin, and Lower Colorado River Authority; this partnership was formed in 1993 to manage Austin-area telecommunications network. The network, which is owned and managed by the partners, consists of over 350 miles of fiber-optic cable connecting more than 500 partner sites. DIR leases dark fiber from GAATN to run the state telecommunications network in Austin, which DIR customers use to access DIR Voice and data services as well as data center connectivity.

¹⁷⁹ [Gov't Code § 2054.003\(9\)](#).

¹⁸⁰ [Gov't Code § 2157.068\(j\)](#); *see also* [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\)](#).

k) If contracted expenditures are made through this program, please provide

A Short Summary of The General Purpose of Those Contracts Overall

The contracts in this program are primarily used for delivering telecommunications services to customers.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$100.1 million in contracted expenditures, the majority of which were funds expended for services consumed by and billed to DIR customers.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 107 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from August 2021 through August 2022 for these contracts. The contracts are funded through amounts billed to and collected from customers and deposited into the telecommunications revolving account.

The Method Used to Procure Those Contracts

The methods used to procure these contracts include direct award, invitation to bid, request for quote, and TXSmartbuy.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-TEX-AN-NG-CTSA-005	AT&T	AT&T provides telecommunications services through this contract, including local voice services, long distance services, internet, metro ethernet, small office/home office (SOHO), and voice over IP (VOIP) services.	\$48,575,439.57
DIR-TELE-CTSA-002	AT&T	AT&T provides telecommunications services through this contract, including local voice services, long distance services, internet, metro ethernet, small office/home office (SOHO), voice over IP (VOIP) services, wireless, NG-911, SD-WAN, as well as conferencing and collaboration services.	\$24,516,673.42
DIR-TEX-AN-NG-CTSA-008	Charter Communications Operating LLC	Charter Communications (on behalf of itself and of its subsidiary, Spectrum Gulf Coast, LLC (formerly known as Time Warner Cable) offers telecommunications services through this contract, including metro ethernet services, internet services, and small office/home office (SOHO) services.	\$5,943,901.36
DIR-TSO-4167	Cisco Systems, Inc.	Cisco Systems offers Cisco branded hardware, networking equipment, servers, data storage solutions, and related services through this contract.	\$4,533,238.10
DIR-CPO-4776	Frank Low Voltage LLC	Frank Low Voltage, LLC offers cabling installation services through this contract, including telecommunication equipment, electrical equipment, cables, wires, and communication and media related services.	\$2,787,961.98

The Methods Used to Ensure Accountability for Funding and Performance

Contracts are assigned Contract Managers who work with program staff to ensure that vendors are delivering services and performing in accordance with the contracts.

A Short Description of Any Current Contracting Problems.

Not applicable.

I) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

Barrier 1: Workforce

As discussed in detail in IX. Major Issues, DIR faces specific recruiting and workforce barriers for the CTS program. Network engineers are particularly difficult to hire as qualified candidates are seeking higher paying roles or roles that are completely remote. Due to this difficulty, the program recently had to fill a vacancy utilizing Telecom Managed Services contracts. If conditions remain the same, DIR may need to explore a managed service solution for the enterprise network or allow engineers to work entirely remotely.

Barrier 2: Outdated Statutory Language

Section IX. Major Issues comprehensively explains DIR's issues with outdated and ambiguous statutory language. For the CTS program, as technology has advanced, some of the statutes are no longer relevant or the statutes have the same outdated meaning as when originally drafted. For example, the Government Code authorizes pay phones in the Capitol Complex and state agency buildings, requiring DIR to report on the revenue received from operation of these phones.¹⁸¹ However, there are no longer pay phones in these buildings.

The Government Code also allows agencies to purchase their own telephones,¹⁸² which made sense when state agencies operated on the now-antiquated PBX system. As DIR has migrated many state agency phones to the VoIP model, DIR now provides phones bundled with voice services and no longer has a model set up to allow agencies to purchase their own phones, rendering the statute obsolete.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

As part of the Biennial Performance Report, [Government Code Section 2054.055\(b\)\(10\)](#)¹⁸³ requires DIR to report on the progress of the plan for a state telecommunications network and the development of a system of telecommunications services as provided by [Government Code Chapter 2054 Subchapter H](#).¹⁸⁴ [Government Code Section 2054.055\(b\)\(1\)](#) requires reports on the performance of the statewide consolidated telecommunications system and the centralized CCTS.¹⁸⁵ The [2022 Biennial Performance Report Telecommunications Report](#) is attached.

¹⁸¹ [Gov't Code § 2170.009](#).

¹⁸² [Gov't Code § 2170.059](#).

¹⁸³ [Gov't Code § 2054.055\(b\)\(10\)](#).

¹⁸⁴ [Gov't Code ch. 2054. subch. H](#).

¹⁸⁵ [Gov't Code § 2054.055\(b\)\(1\)](#).

- o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility).

Not applicable.

- p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Cybersecurity



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, **protecting state technology infrastructure**, and offering innovative and cost-effective solutions for all levels of government.

- a) Provide the following information at the beginning of each program description.

Name of Program or Function: Cybersecurity

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701
Network Security Operation Center

Contact Name: Nancy Rainosek, Chief Information Security Officer
Dale Richardson, Chief Operations Officer

Statutory Citation for Program:

[Education Code Section 11.175, School Cybersecurity](#)

[Government Code Chapter 2054, Subchapter C, General Powers and Duties of Department](#)

[Government Code Chapter 2054, Subchapter F, Other Powers and Duties of State Agencies](#)

[Government Code Chapter 2054, Subchapter L, Statewide Technology Centers](#)

[Government Code Chapter 2054, Subchapter N-1 Cybersecurity](#)

[Government Code Chapter 2054, Subchapter N-2 Texas Volunteer Incidence Response Team](#)

[Government Code Chapter 2059, Texas Computer Network Security System](#)

[General Appropriations Act FY22-23 Article IX Section 18.37 - Contingency Rider for Senate Bill 475](#)

[House Bill 5 – Supplemental Bill, 87th 2nd Called Special Session](#)

[House Bill 2 – Supplemental Bill, 87th 2nd Called Special Session](#)

- b) What is the objective of this program or function? Describe the major activities performed under this program.

Texans entrust their private data to state government entities and DIR's top priority is to

protect that data and Texas' technology infrastructure from the growing threat of cyberattacks that seek to disrupt the continuity of government. To ensure that Texans' data is protected and that government services remain secure and available, DIR's Cybersecurity function is woven throughout the agency and given top consideration in all agency matters.



The objectives of DIR's Cybersecurity function are to:

- Protect the state's technology infrastructure from cyber threats by detecting and counteracting malicious network activity;
- Respond and offer immediate assistance to government entities during a cybersecurity incident;
- Adopt a whole-of-state approach as partners in securing the state's infrastructure by developing a strategy and preparedness plan; and
- Safeguard Texans' information, data, and privacy by providing leadership, training, guidance, accountability, consultation, and promotion of cybersecurity best practices.

DIR achieves these objectives through the following major activities, which are classified into three categories:

- Cybersecurity Protection, Prevention, and Response;
- Cybersecurity Policies and Guidance; and
- Cybersecurity Training and Outreach.

Cybersecurity Protection, Prevention, and Response

Texas is an alluring target for cyber threat actors due to its growing population, economic activity, critical infrastructure, and political climate. DIR is committed to preventing and protecting against cybersecurity incidents in Texas. DIR develops initiatives and programs to combat cyber threat actors and keep Texans (and their sensitive data) secure.

DIR performs the following Cybersecurity Protection, Prevention, and Response major activities.

Responding to and Helping Mitigate Cybersecurity Incidents for Texas Entities, Including State Agencies and Local Government Entities

- DIR's **Cybersecurity Incident Response Team (CIRT)** provides eligible entities with onsite or remote cybersecurity incident support to help recover from or remediate cyberattacks. The CIRT also notifies government entities of vulnerabilities or compromises discovered through intelligence gathering.
- DIR directs the **Volunteer Incident Response Team (VIRT)**, which is a team of volunteers with expertise addressing cybersecurity incidents and providing rapid cybersecurity incident response assistance if the cybersecurity incident affects multiple participating entities or is declared a disaster by the Governor. The VIRT currently comprises 102 volunteers across the state of Texas.

- DIR operates the **Regional Security Operations Centers (RSOCs)** in partnership with selected public universities to provide cybersecurity services to local entities. The RSOC program offers security monitoring, alerting, guidance, training, and protection to help local entities prevent and rapidly recover from cybersecurity incidents. University students can work at the RSOCs and receive hands-on experience, strengthening the cybersecurity workforce of tomorrow. DIR partnered with Angelo State University to operate the pilot RSOC in 2022 and will add two more RSOCs in 2023 at the University of Texas at Austin and at the University of Texas Rio Grande Valley.
- DIR leads and coordinates statewide efforts to response and recovery in a cybersecurity disaster as defined by the **Texas Division of Emergency Management (TDEM) Cybersecurity Annex**.

Monitoring and Defending Texas' Network via the Network Security Operations Center (NSOC)

- DIR provides **24-hour continuous network security** system services for all state agencies.
- DIR **blocks malicious inbound network traffic**, alerts agencies of suspicious outbound traffic, and mitigates distributed denial-of-service (DDoS) attacks.
- DIR manages the development, coordination, and execution of **statewide cybersecurity operations** to isolate, contain, and mitigate the impact of network security incidents.

It is important to note that the Government Code¹⁸⁶ prescribes that if DIR provides network security services for a state agency or other entity, then DIR is responsible for network security from external threats for that agency or entity. Network security management for that state agency or entity regarding internal threats remains the responsibility of that state agency or entity.

Providing Security Services, Tools, Expertise, and Support to Eligible Public Entities

- DIR offers **Managed Security Services (MSS)** through the Shared Technology Services (STS) program to assist eligible customers in consolidating security services, meeting legislative security requirements, and mitigating security risks. MSS consists of three main service components: Security Monitoring and Device Management (SMDM), Incident Response, and Risk and Compliance. Each component contains a subset of security-related services that customers can choose from to meet their security needs. DIR contracts with a third party to provide MSS.

¹⁸⁶ [Gov't Code § 2059.056](#).

- DIR manages the statewide **Multi-factor Authentication (MFA) program**, which provides state agencies and institutions of higher education with identity and access management (IAM) services at low to no cost.
- DIR conducts **security assessments and penetration tests** for state agencies, institutions of higher education, and public junior colleges.
- DIR provides state agencies and institutions of higher education **endpoint detection and response (EDR)** at no cost to protect state-issued computers, laptops, servers, and other endpoints from ransomware and other cyber threats.

Sharing Cybersecurity Intelligence Materials, Including Threat Intelligence, Forensic Analysis Reports, White Papers, Cybersecurity Bulletins, Risk Letters, and More

DIR administers the **Texas Information Sharing and Analysis Organization (TX-ISAO)**, a forum for Texas public and private sector entities to collect and share cybersecurity threat intelligence. DIR hosts monthly TX-ISAO meetings and distributes newsletters.

Cybersecurity Policies and Guidance

Texas' cybersecurity landscape is constantly changing. To combat the unpredictable cybersecurity landscape, DIR provides policies and guidance so that all state agencies and institutions of higher education adopt a uniform approach to protecting critical state information assets. State agencies and local government entities rely on DIR for clear guidance and policies to protect against cyber threat actors with increasingly sophisticated tactics and growing resources.

DIR performs the following Cybersecurity Policies and Guidance major activities.

Establishing Security Rules and Standards for State Agencies

- DIR sets administrative rules establishing information security standards at [1 Texas Administrative Code Chapter 202](#), defining information security standard requirements for state agencies, institutions of higher education, and public junior colleges.¹⁸⁷
- DIR established and now maintains the **Security Controls Standards Catalog**, which defines the minimum technical and administrative security control requirements for state information systems.
- DIR developed and now maintains the **Texas Cybersecurity Framework** to provide a context for evaluating the current and historical maturity of an entity, and help organizations identify, assess, and manage cybersecurity risks in their environments against a standardized set of information security functions and areas of focus.

¹⁸⁷ [1 Tex. Admin. Code Chapter 202](#).

Setting Criteria to Minimize Cybersecurity Threats Imposed by Vendors and Products

- DIR established and oversees the **Texas Risk and Authorization Management Program (TX-RAMP)**, which certifies cloud computing services for state agencies and institutions of higher education.
- DIR maintains the list of **prohibited technologies** for use on state-owned and leased devices.

Collecting and Managing Required Information from State Agencies, Vendors, and Other Entities for Compliance with Statutorily Required Reports and Programs

DIR administers the **Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM)**, a software portal to collect security-related information. The portal is a central repository of information relating to security incidents, security services, security plans, and various other optional and required tools to assist entities with maturing their approach to information security management. SPECTRIM currently allows agencies to report urgent security incidents to DIR, perform risk assessments on their information assets, assess and monitor enterprise-defined information security risks, report information required for statutory reports, and more.

Providing Comprehensive Plans, Reports, and Analyses Concerning Texas' Cybersecurity Posture

- Through the **Biennial Information Security Report**, DIR analyzes the data reported by state agencies to identify cybersecurity trends and report on the statewide security posture with recommendations for improving areas of deficiency.
- Through the **Biennial Cybersecurity Report**, DIR identifies the resources currently available to government entities to respond to cybersecurity incidents, evaluates the information security resource sharing program, and provides legislative recommendations for improving the cybersecurity posture of the state.
- In the **Annual Nationwide Cybersecurity Review (NCSR)**, DIR conducts a self-assessment of the state's level of cybersecurity maturity in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework functions.
- In the **Homeland Security Strategic Plan – Agency Implementation Plan**, DIR supports the execution of the state's five-year Homeland Security Strategic plan and creates an annual agency implementation plan to align statewide cybersecurity incident response activities with the state's homeland security goals.
- DIR develops and maintains a **Statewide Cyber Incident Response Plan** in conjunction with members of the Statewide Incident Response Workgroup to address the technical considerations of preparing for and responding to cybersecurity incidents and establish a procedure for deploying state resources in the event of a cybersecurity incident.

Providing Cybersecurity Leadership and Guidance and Developing Cybersecurity Best Practices

- DIR leads the **Texas Cybersecurity Council**, a statutorily created group that includes public and private sector leaders and cybersecurity employees who collaborate on and develop best practices for cybersecurity matters in Texas and provide legislative recommendations to address cybersecurity issues.¹⁸⁸
- DIR leads the **State Information Security Advisory Committee (SISAC)**, which includes state and local government information security professionals that meet monthly to share ideas and best practices and make recommendations to DIR for more effective information security operations among and within government entities. This committee also provides input regarding the minimum information security standards and statewide policies and guidance.
- DIR established a framework for **regional cybersecurity working groups** to execute mutual aid agreements that allow state agencies, local governments, regional planning commissions, public and private institutions, the private sector, and the Volunteer Incident Response Team (VIRT) to assist with responding to a cybersecurity incident.
- DIR offers the **Texas Cyberstar Certificate**, a statutorily authorized program recognizing public and private entities in Texas who implement cybersecurity best practices.¹⁸⁹ To date, 18 entities have earned the Cyberstar Certificate.

Cybersecurity Training and Outreach

DIR keeps Texans' information safe and secure by providing frequent and consistent opportunities for cybersecurity training and outreach to state agencies, institutions of higher education, and local governments.

DIR performs the following Cybersecurity Training and Outreach major activities.

Managing Texas' Mandatory Cybersecurity Awareness Training Program for State and Local Entities

- DIR **annually certifies cybersecurity training programs**, updates standards for maintenance of certification, and oversees the compliance reporting for state and local entities.¹⁹⁰
- DIR also funds and provides certified **end user awareness training** to state agencies, universities, and public junior colleges.

¹⁸⁸ [Gov't Code § 2054.512.](#)

¹⁸⁹ [Gov't Code § 2054.5181.](#)

¹⁹⁰ [Gov't Code § 2054.519 – 2054.5192.](#)

Facilitating Training and Outreach Events, Including Tabletop Exercises, Incident Response Plan Development Trainings, and Conferences

- DIR provides free training for state agency cybersecurity and IT staff through the **InfoSec Academy and Secure Developer Training Program**.
- DIR organizes and hosts the annual **Information Security Forum (ISF)**, a premiere cybersecurity conference featuring multiple developmental tracks and breakout sessions.
- DIR coordinates, organizes, and hosts bi-monthly **educational webinars**, DIR monthly webinars, Gartner monthly webinars, monthly Texas Information Sharing and Analysis Organization (TX-ISAO) meetings, and Statewide Information Security Advisory Committee (SISAC) meetings.
- DIR maintains the Statewide Cyber Incident Response Plan and Statewide Incident Response Workgroup.
- DIR promotes and participates in **Texas' Cybersecurity Awareness Month** in October by organizing and supporting activities and posting to social media about best practices for cyber hygiene.
- DIR provides **incident response plan development trainings** on the DIR Incident Response Team Redbook to eligible customers.
- DIR conducts personalized **cybersecurity incident response simulation exercises** (tabletops) to eligible customers.

Providing Best Practices and Resources for Texans, Increasing the Cybersecurity Posture of the State

- From best practices when shopping online to advice on how to protect privacy when using mobile apps, DIR publishes **cybersecurity tips and tools for Texans** on the [Cyber Safety Corner of Texas.gov](#) that raise awareness on how Texans can take steps to keep themselves safe online.
- DIR's website shares strong **cybersecurity best practices** intended to help Texans protect their personal information and practice good cyber hygiene:
<https://dir.texas.gov/cybersecurity-information-texans>.

c) What information can you provide that shows the effectiveness and efficiency of this program or function? If applicable, reference but do not repeat any performance measures from Section II, Exhibit 2, and provide any other metrics of program effectiveness and efficiency. Also, please provide the calculation or methodology behind each statistic or performance measure.

DIR maintains several key metrics that reflect the effectiveness and efficiency of each of its Cybersecurity function objectives. For convenience, these metrics have been divided by major activity performed.

Cybersecurity Protection, Prevention, and Response

Monitoring and Defending through the Network Security Operation Center (NSOC)

DIR manages the network security system services for all state agencies receiving internet service through the NSOC, which maintains real-time network security monitoring to detect and respond to network security events. To accomplish these responsibilities, DIR implements best-of-breed cybersecurity technologies and services. DIR team members use these technologies and services to block unwanted or threatening network traffic, alert agencies to suspicious network traffic, detect and mitigate distributed denial-of-service (DDoS) attacks, and perform network security forensics.

DIR creates a monthly report for the Office of the Governor containing metrics on:

- Total number of perimeter blocks;
- Most frequent attacking countries;
- Most frequently targeted agencies;
- Most frequent filters triggered;
- Alerts by cyber threat variant;
- Alert notifications sent to agencies;
- Phishing emails entities reported to DIR (and resulting counter measures);
- The threat level of differing cyber threat actor organizations; and
- Immediate threats DIR is tracking.

Attached is an example of this report, which contains network security information that DIR considers to be confidential information under Government Code [Chapter 552](#).

The charts below display the NSOC metrics for monthly blocks, alerts sent to agencies, and distributed denial-of-service (DDoS) attack alerts in the past two fiscal years.

Figure 26 Total Logged Blocks by Month



Figure 27 Total Alert Notifications Sent to Agencies

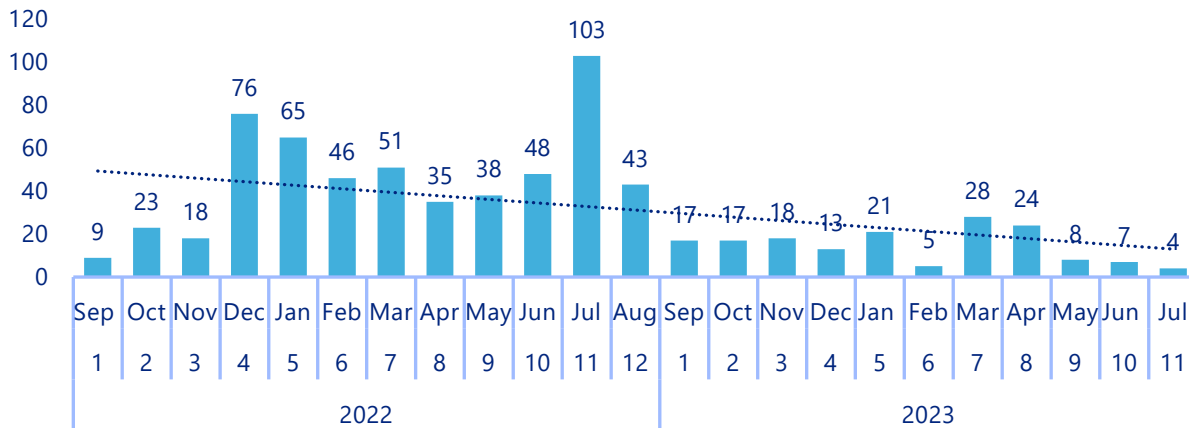
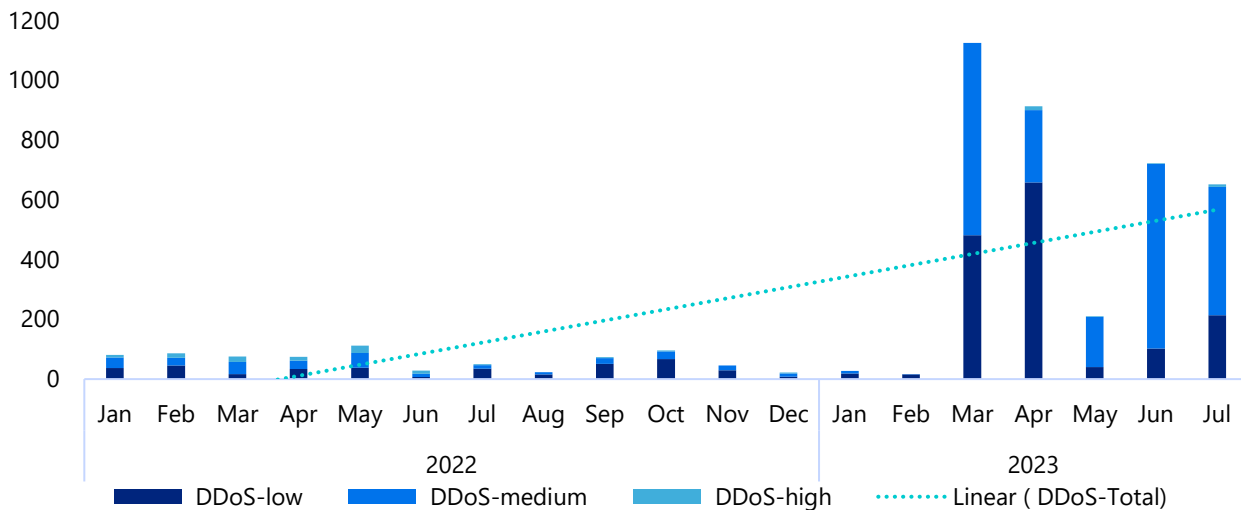


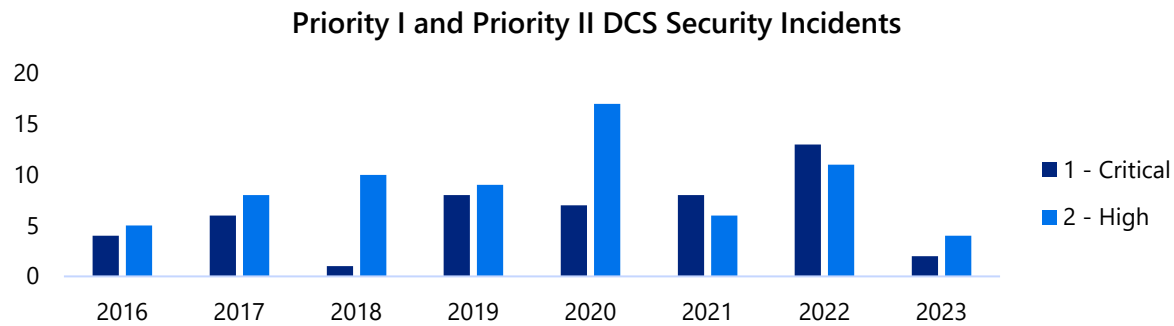
Figure 28 Distributed Denial-of-Service (DDoS) Alerts



Mitigating Data Center Services Incidents

DIR oversees cybersecurity operations in the Shared Technology Services (STS) Data Center Services (DCS) program. DIR responds to all major security incidents in DCS and provides guidance and support for customers connected to the DIR network. The following chart shows the DCS program’s Priority I (Critical) and Priority II (High) security incidents since 2016.

Figure 29 Priority I and Priority II DCS Security Incidents



Responding to Local Government Entities

DIR responds to state and local entities experiencing cybersecurity incidents. Since 2020, DIR has provided support and guidance for more than 90 ransomware incidents, including five incidents requiring onsite deployments.

Administering the Regional Security Operations Center (RSOC)

Since its implementation in 2022, the Angelo State University RSOC has onboarded 18 entities with 18 additional interested entities applied and waitlisted to join the RSOC. This pilot RSOC is currently monitoring 3,009 non-server endpoints and 77 server endpoints. As of May 2023, the San Angelo RSOC has enlisted 24 Student Cybersecurity Analysts who will progress through various tiers of cybersecurity college courses.

Providing Security Services, Tools, Expertise, and Support

Endpoint detection and response (EDR) - DIR oversees the daily operations of the state-funded EDR service, which provides endpoint protection and active response under DIR’s Managed Security Services (MSS) program. The EDR program is currently monitoring and protecting over 100,000 computing devices and has thwarted over 49,000 cyber threats.

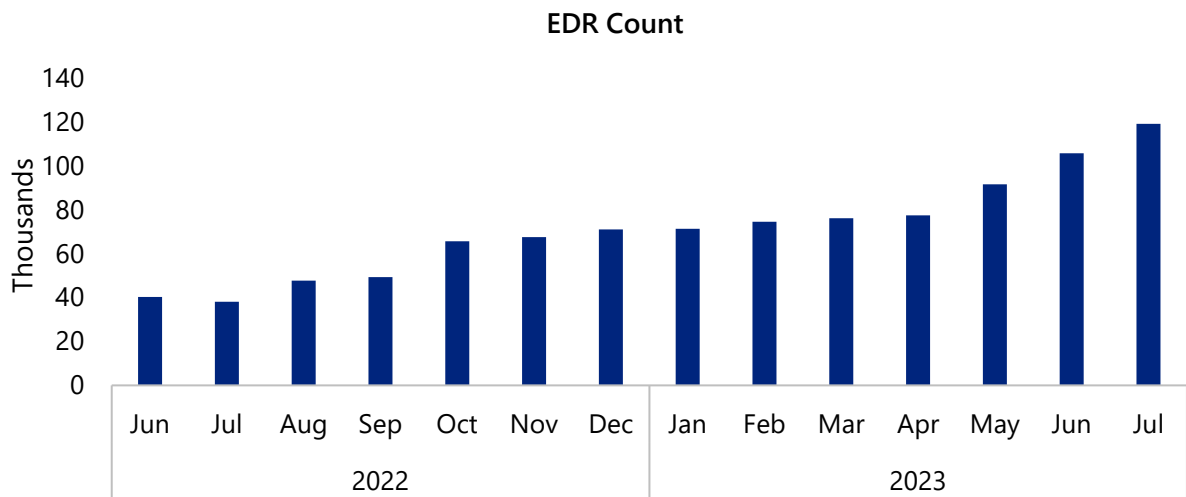
The table below summarizes the number of endpoints protected and cyber threats detected and mitigated in July 2023.

Figure 30 July 2023 EDR Summary

July 2023 EDR Summary	
Device Count	119,176
July Threat Count	4,860
Total Threat Count	49,639

The following chart shows the number of endpoints DIR’s EDR program protects each month.

Figure 31 EDR Count



Statewide Risk-Based Multifactor Authentication (MFA) – DIR’s MFA program, known as the Texas Digital Identity Solution (TDIS), provides a voluntary service with a specific set of identity and access management (IAM) features. The service is available to state agencies and institutions of higher education.

The MFA program currently serves:

- 74,953 active users with 31,200 users in the process of being added.
- 10 customers provided MFA directly and to users of the Texas Comptroller of Public Accounts’ Centralized Accounting and Payroll/Personnel System (CAPPS), the Shared Technology Services Portal, and the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM).
- Four MFA projects in process, including two that will begin in early 2024. DIR is also planning an additional seven projects.

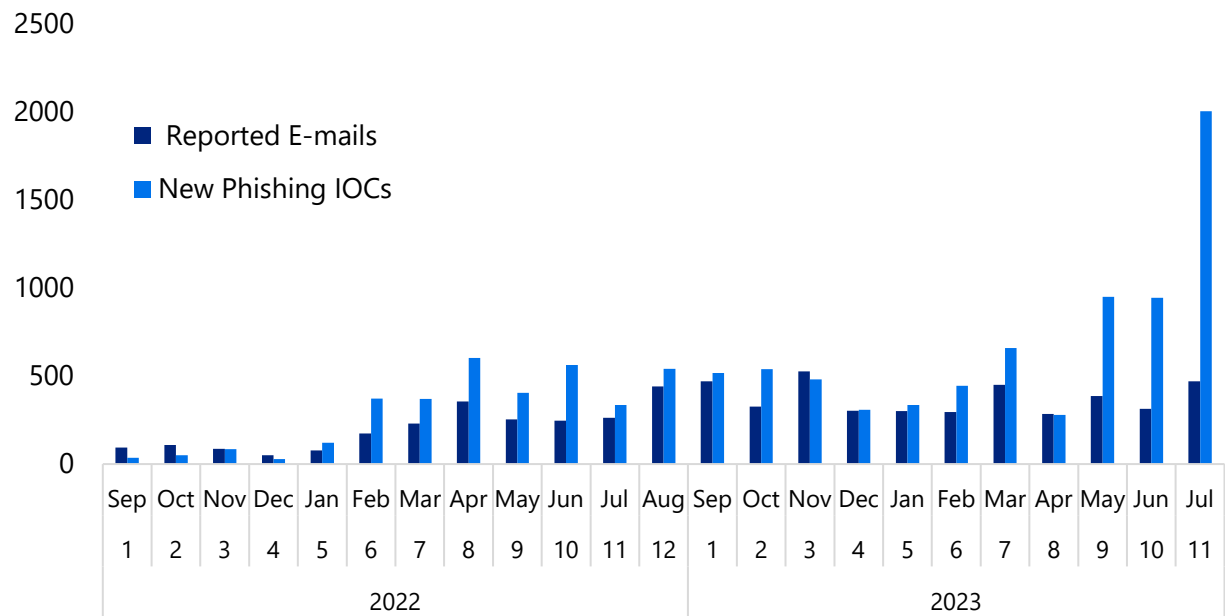
Sharing Cybersecurity Intelligence Notification and Materials

DIR is constantly adding threat intelligence to the security toolset that protects the state’s network, and on average, intakes 5,000 new indicators of compromise (IOCs) daily. IOCs include internet protocol (IP) addresses, domain names, Uniform Resource Locators (URLs), and file hashes that can indicate malicious activity on the network. Additionally, state agencies send suspicious emails to DIR for DIR’s Cybersecurity Analysts to safely and security analyze using DIR’s tools. DIR’s Cybersecurity Analysts add any IOCs collected from these emails to the DIR toolsets for malicious network traffic blocking and alerting purposes. DIR adds the IOCs from both the toolsets and those collected from agencies’ reported emails to a weekly report that is shared with the Texas Information Sharing and Analysis Organization (TX-ISAO) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The chart below shows a comparison of the number of phishing emails analyzed each month to

the number of IOCs that were harvested via DIR analysis. (DIR implemented deep analysis tools in mid-January 2022, resulting in the ability to collect additional IOCs).

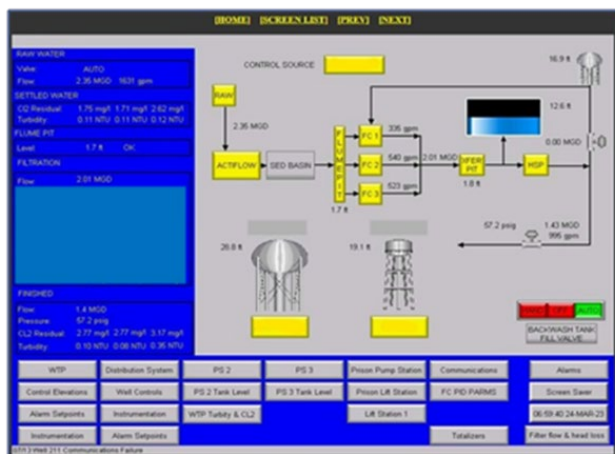
Figure 32 Phishing Emails Analyzed per Month



DIR’s Cyber Threat Researchers search the dark web and other intelligence sources for information on compromises at Texas entities. The team then proactively notifies the entities of their findings on vulnerabilities such as compromised login credentials, provides support for events such as web defacements, and responds to requests for technical assistance such as digital forensics.

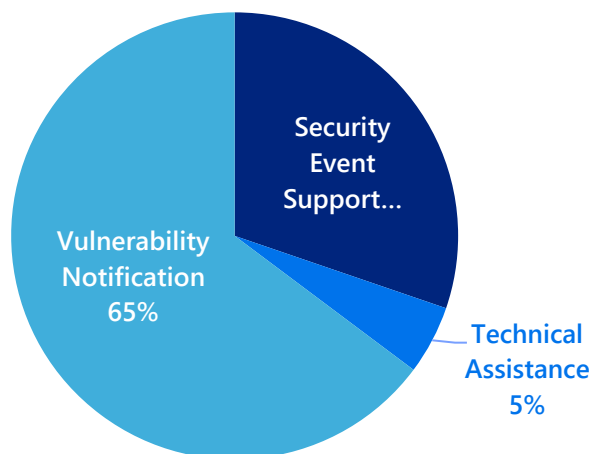
For example, a DIR Cyber Threat Researcher found the below screen capture of a supervisory control and data acquisition (SCADA) system for a Texas entity’s water supply that was unintentionally accessible via the internet. DIR contacted the entity to notify the vulnerable entity of the risk and advised them to remove remote access to the system before cyber threat actors could cause damage.

Figure 33 Screen Capture of a Supervisory Control and Data Acquisition (SCADA) System



This example is one of the 281 vulnerabilities or system compromises that DIR discovered on the dark web or other intelligences sources (with the vulnerable entity notified) in the past two years. The below chart details the type of breakdown of these notifications.

Figure 34 Vulnerabilities or System Compromises Chart

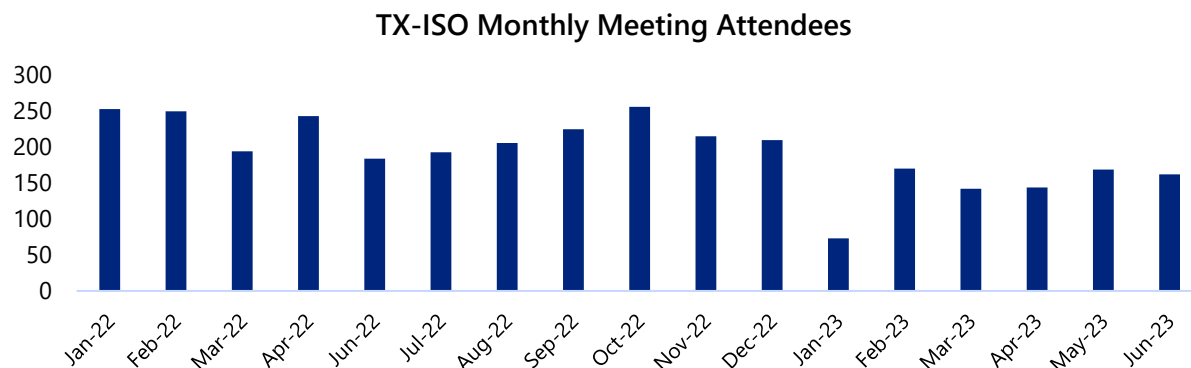


Operating the Texas Information Sharing and Analysis Organization (TX-ISAO)

DIR operates the TX-ISAO to provide a forum for entities in Texas to share information regarding cybersecurity threats, best practices, and remediation strategies.

The TX-ISAO is open to any entity in Texas, including state agencies, local governments, public and private institutions of higher education, and the private sector. The TX-ISAO counts 1,958 members as of June 2023 and averages 193 attendees at its monthly meetings. The chart below reflects participation in the TX-ISAO's monthly meetings.

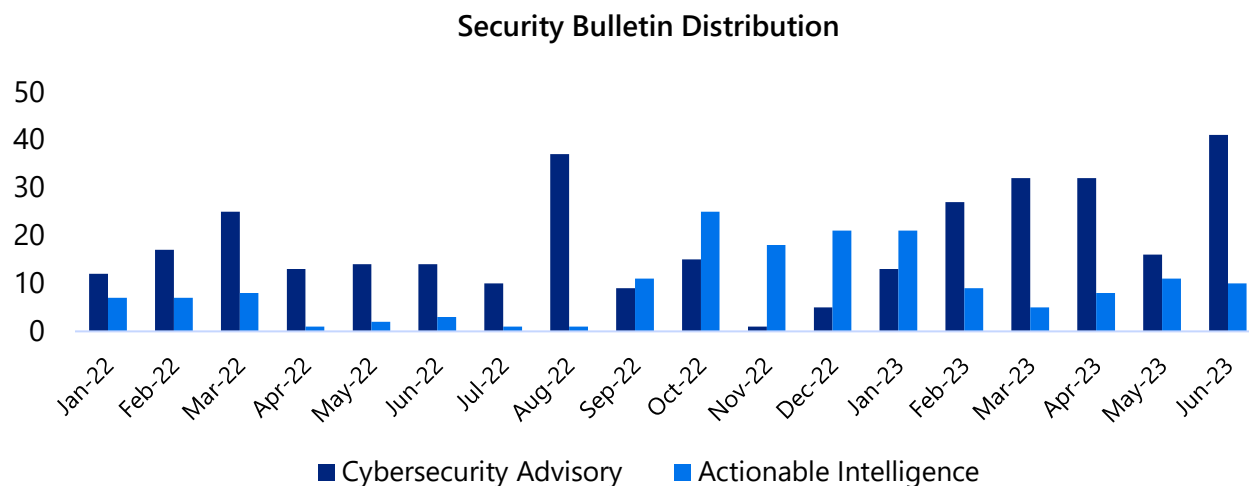
Figure 35 TX-ISAO Monthly Meeting Attendees



Since January 2022, the TX-ISAO has distributed the following:

- 333 cybersecurity advisories (general guidance that entities can act on to mitigate the risk of cybersecurity attacks) reflected in the chart below;
- 169 actionable intelligence notifications (specific intelligence with information about a known vulnerability) reflected in the chart below;
- Two white papers; and
- Seven high-priority cybersecurity advisories, including eight additional updated versions.

Figure 36 Security Bulletin Distribution



Cybersecurity Policies and Guidance

Measuring State Agency Maturity Growth

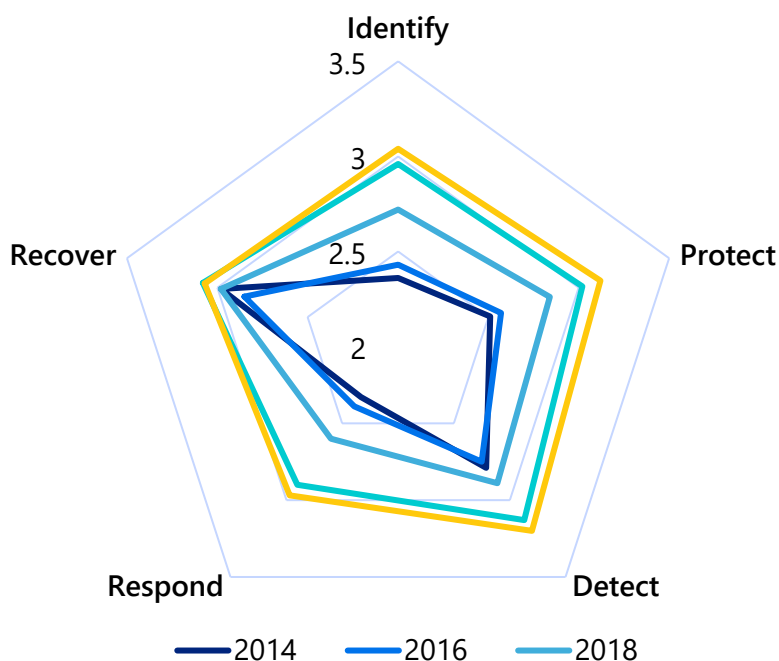
DIR is charged with assisting state agencies in improving their cybersecurity programs and improving the state of security for Texas as a whole. In 2014, DIR developed the Texas Cybersecurity Framework (TCF), which creates a common language by which state agencies can measure their security in five categories.

State agencies conduct a self-assessment of their security maturity on a biennial basis during the agency security planning process. These self-assessments reflect consistent growth in maturity against TCF categories since the initial implementation of the TCF in 2014. The TCF is intended to help organizations better understand, manage, and reduce cybersecurity risks. Part of the structure is determining the maturity of each security control objective. The term “maturity” relates to the degree of implementation and optimization of processes, from ad hoc practices all the way up to active optimization of the processes. Entities are scored from zero to five based on maturity, and agencies should strive for a minimum maturity score of 3, which is associated with having a defined and compliant approach to a given security objective. The following information explains each score:

- 0 – None, Nonexistent. There is no evidence of the organization meeting the objective.
- 1 – Ad hoc, Initial. The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
- 2 – Consistent, Repeatable. The organization has a consistent overall approach to meeting the objective but is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
- 3 – Compliant, Defined. The organization has a documented, detailed approach to meeting the objective, and regularly measures compliance.
- 4 – Risk-based, Managed. The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
- 5 – Efficient, Optimized. The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

The chart below provides high-level, collective insight into the benefits of enterprise information security initiatives and services.

Figure 37 Functional Area Maturity 2014-2022



Funding Security Assessments and Penetration Tests

DIR funds security assessments, including TCF assessments, penetration tests, and web application penetration tests for state agencies, institutions of higher education, and public junior colleges. The TCF assessments ensure alignment with cybersecurity best practices and controls and include recommendations and action plans to improve the entity's cybersecurity posture. Penetration tests identify weaknesses in system configurations and network infrastructure that may lead to data breaches and malicious attacks. Once concluded, penetration tests identify ways for the entity to amend their systems, networks, or security protocols to overcome security gaps.

This combination of testing and assessments provides state agencies with well-rounded visibility into the security of their current environment, which guides them towards improvement. The chart below reflects the DIR-funded testing for state agencies, institutions of higher education, and public junior colleges in FY22 and FY23.

Figure 38 DIR-Funded Testing

Test Type	FY22	FY23 (As of August 1)
Texas Cybersecurity Framework (TCF) Assessments	45	35
Penetration Tests	66	58
Web Application Penetration Tests	13	8

Minimizing Cybersecurity Threats Imposed by Third-Party Vendors and Products

The Texas Risk and Authorization Management Program (TX-RAMP), created by [Senate Bill 475](#), requires DIR to establish a program to evaluate and certify cloud computing services that

process the data of state agencies, public institutions of higher education, and public junior colleges.¹⁹¹ To obtain a TX-RAMP certification, vendors of cloud computing services request an assessment from DIR in which DIR reviews security information regarding the product to ensure a standardized security approach. DIR may also accept confirmation from other federal, state, or authorized programs indicating the product's receipt of another risk and authorization management program's certification.

The chart below reflects the requests for TX-RAMP assessments and certifications issued since the program began in December 2021.

Figure 39 TX-RAMP Assessments and Certifications

TX-RAMP Assessment Requests and Certifications	
Assessment Requests Processed	2,450
Cloud Services Certified under TX-RAMP	1,837

Cybersecurity Training and Outreach

Overseeing Texas' Mandatory Cybersecurity Awareness Training Program

DIR is required by statute to annually certify a minimum of five security training programs and publish a complete list of these certified cybersecurity training programs to the DIR website. State agencies and local government staff who use a computer for 25 percent or more of their duties must utilize one of these certified security training programs to annually complete their required cybersecurity training.

Figure 40 Cybersecurity Training and Compliance

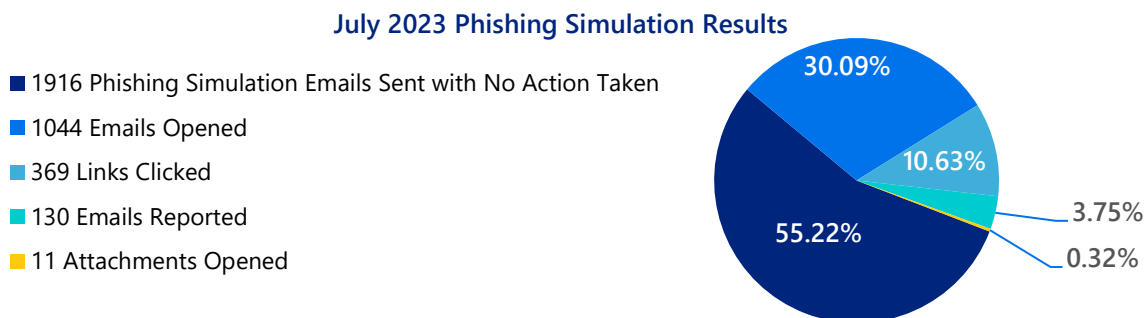
Number of Cybersecurity Training Programs DIR Certified in FY22	160
Number of Cybersecurity Training Compliance Reports DIR Received for FY22	2,559

Executing End User Security Awareness Training/Phishing Simulation

DIR currently provides 677 organizations with security knowledge and awareness training through the DIR-funded Security Awareness Training Program, including 12 institutions of higher education, 24 public junior colleges, and 41 state agencies. Through reporting, DIR can identify and incorporate key performance indicators (KPIs) to track participation and performance. Examples of KPIs include emails sent, emails opened, click rate, and report rate. The chart below shows results from the July 2023 phishing email campaign that sent fake phishing emails to test employees' awareness of malicious tactics.

¹⁹¹ [Acts 2021, 88th Leg., R.S., ch. 567 \(S.B. 475\), §§ 2, 11 \(codified at Gov't Code § 2054.0593\).](#)

Figure 41 July 2023 Phishing Simulation Results



Facilitating Other Trainings

The Texas InfoSec Academy is a DIR-funded program that helps state agencies and institutions of higher education prepare their IT and security staff to meet today's challenges by providing industry-standard cybersecurity certification examination preparation courses and exam vouchers. In addition, the InfoSec Academy offers secure coding training to state agency application developers. Courses in the InfoSec Academy are high-caliber training opportunities. Tuition for these training courses ranges from \$1,000 up to \$3,960, more than many agencies would be able to afford without DIR funding the program. DIR also provides a certification voucher at no cost to eligible customers.

The chart below shows InfoSec Academy program metrics since 2018.

Figure 42 InfoSec Academy Program Metrics

Total number of individuals trained	1,074
Total number of courses funded	1,752
Total number of certification exam vouchers issued	1,051

DIR contracts with Gartner to jointly host monthly webinars tailored for public sector employees that focus on current cybersecurity trends and topics. Gartner webinars are one-hour engagements organized by DIR and include presentations by nationally recognized experts in cybersecurity. These monthly webinars cover a variety of topics, including new threat vectors, mitigation and containment tools, trends in global political climate that are likely to affect cybersecurity matters, and the future state of cybersecurity. The average attendance at each of these webinars, including Gartner monthly webinars and the Office of the Chief Information Security Officer (OCISO) bi-monthly webinar, is 56 participants.

DIR conducts the annual Information Security Forum (ISF), a two-day cybersecurity conference that hosts between 400 – 500 attendees and approximately 100 exhibitors. The 2023 ISF hosted 461 attendees and received an 8.3 overall satisfaction rating on a scale of one to 10, according to a post-event survey.

Figure 43 Organization Type Breakdown

Organization Type Breakdown	
City	38
Higher Ed	54
Junior College	10
K-12	40
State Agency	250
Other Gov't	13

In 2022, the ISF hosted 423 attendees and received an overall satisfaction rating of 8.97, according to a post-event survey.

d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

Securing state agency data, information security resources, and continuity of operations became additional DIR core functions at the beginning of the 21st century as Texas government moved online and recognized DIR's unique position as the technology agency capable of addressing the risks associated with this transition. In 2001, the Legislature established a statewide security program at DIR, which it first funded in 2006, appropriating \$5.7 million to DIR for the biennium. As cyber threats have increased, the Legislature has recognized the importance of cybersecurity and affirmed its trust in DIR to focus on this critical issue by increasing DIR's cybersecurity funding to \$103 million in 2025-2026, expanding DIR's responsibility to oversee cybersecurity in Texas.

DIR breaks down the history of its Cybersecurity function into two sections:

- Significant Legislation and Budget Authority; and
- Significant Cybersecurity Events.

Significant Legislation and Budget Authority

2005 – 79th Texas Legislative Session

HB 3112 - HB 3112 enacted Government Code Chapter 2059, requiring DIR to establish a secure network security center and provide network security services to state agencies.

Implementation: Following the passage of HB 3112 in 2005, DIR converted the previous Disaster Recovery Operations Center (DROC) into the Network Security Operations Center (NSOC). DIR oversaw contracted analysts providing network security during business hours and managed tools monitoring the network around the clock. In 2012, DIR became actively involved in the day-to-day operations, adding in-house DIR NSOC Manager and DIR Cybersecurity Analysts. On March 1, 2018, the NSOC security services contract was transitioned to the new Managed Security Services (MSS), and DIR took ownership of the tools. The MSS contract was amended in 2019 to extend the manned coverage to 5 a.m. – 9 p.m. weekdays and added limited weekend coverage. In December 2020, DIR amended the MSS contract to provide

manned coverage around the clock. Today, DIR Cybersecurity Analysts oversee the contractor analysts, document processes and procedures, conduct dark web investigations, perform advanced threat hunting, operate threat intelligence gathering and sharing, and manage the DIR security tools. In 2021, the Legislature amended Government Code Chapter 2059 to authorize the creation of the Regional Security Operations Center (RSOC), discussed below under SB 475's implementation.

2013 – 83rd Texas Legislative Session

SB 1102 – SB 1102 created the State Cybersecurity Coordinator position under DIR to oversee cybersecurity matters in Texas and authorized this position to establish the private-industry government council to collaborate on cybersecurity matters in Texas.¹⁹²

Implementation: Following the passage of this bill in 2013, DIR designated its Chief Information Security Officer to oversee all cybersecurity matters, including those delegated to the Cybersecurity Coordinator position, for the state. As the Legislature expanded the duties of the State Cybersecurity Coordinator position and DIR's own role in the cybersecurity field, DIR identified a need for a unique full-time employee to address the statutorily identified elements of this role. In 2018, DIR hired the first State Cybersecurity Coordinator and has been funding this position (and certain initiatives associated with it) using State Homeland Security Grant Program funds from the Federal Emergency Management Agency (FEMA). The State Cybersecurity Coordinator now supervises a team of two that oversee the Texas Cybersecurity Council, the Texas Information Sharing and Analysis Organization (TX-ISAO), mandatory statewide cybersecurity training, and the Texas Cyberstar program. The State Cybersecurity Coordinator travels throughout Texas to bring government and business leaders together as partners in securing the state's infrastructure and developing a strategy and plan to promote the cybersecurity industry within the state. Since January 2022, the State Cybersecurity Coordinator has met with 24 groups throughout Texas.

SB 1134 – SB 1134 charged DIR with developing strategies and a framework to secure state agencies' cybersecurity infrastructure, and for a cybersecurity risk assessment and mitigation planning. In addition, DIR was tasked with providing training on cybersecurity measures and awareness, and assistance upon request to state agencies on the strategies and framework that DIR developed.¹⁹³

Implementation: DIR developed and implemented the Texas Cybersecurity Framework (TCF) and implemented the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) to give agencies an automated approach to assessing risks to their information systems.

¹⁹² [Acts 2013, 83rd Leg., ch. 32 \(S.B. 1102\), § 2 \(codified at Gov't Code Chapter 2054, Subchapter O\).](#)

¹⁹³ [Acts 2013, 83rd Leg., ch. 477 \(S.B. 1134\), § 1 \(codified as an amendment to Gov't Code § 2054.059\).](#)

2017 – 85th Texas Legislative Session

HB 8 – The Texas Cybersecurity Act was an omnibus bill aimed at expanding cyber and data security protections in Texas. Critically, the Texas Cybersecurity Act required state agencies to notify DIR, including the Chief Information Security Officer and State Cybersecurity Coordinator, of certain types of security breaches or exposures, in addition to requiring DIR to develop a plan to address cybersecurity risks and incidents in Texas. The act directed DIR to establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies; renamed the private-industry government council to the Texas Cybersecurity Council, and established a set membership roster and statutory goals for the Council; added state agency reports required for submission to DIR to include a biennial information security assessment and report, and a biennial data security plan for online and mobile applications if the state agency is developing an online or mobile application; and expanded the scope of a state agency's legacy systems mitigation and remediation plan as well as that of its vulnerability report. The act also enabled state agencies to receive reimbursement for industry standard cybersecurity certifications.¹⁹⁴

Implementation: Notification of cybersecurity incidents to DIR was already included in [1 Texas Administrative Code Chapter 202](#).¹⁹⁵ The language in HB 8 merely added this provision to the Government Code. DIR had already established a method for reporting incidents through SPECTRIM. DIR renamed the Texas Cybersecurity Council (formerly the Private Industry-Government Council) in 2017 to develop enduring partnerships between private industry and public sector organizations. The council meets bi-monthly and currently counts 18 members that include representatives from the Office of the Governor, Texas Senate, Texas House of Representatives, Elections Division of the Secretary of State, institutions of higher education, and private sector. The council's primary focus is to:

- Ensure that critical infrastructure and sensitive information are protected;
- Develop a cybersecurity workforce to protect technology resources from increasing threats; and
- Develop strategies and solutions to ensure that Texas continues to lead in areas of cybersecurity.

The council produces a biennial report that provides legislative recommendations on any legislation necessary to implement cybersecurity best practices and remediation strategies for Texas.

The Statewide Incident Response Workgroup formed in 2017 and is a collaboration between DIR, the Texas Military Department, the Texas Department of Public Safety, and the Texas

¹⁹⁴ [Acts 2017, 85th Leg., R.S., ch. 683 \(H.B. 8\), 2017 Tex. Gen. Laws 3027 \(codified as an amendment to Government Code Chapter 2054\).](#)

¹⁹⁵ [1 Tex. Admin. Code Chapter 202.](#)

Division of Emergency Management. The Workgroup is responsible for developing a plan to address cybersecurity risks and incidents in Texas and establishes a procedure for deploying state and federal resources in response to local cybersecurity incidents. This collaboration among state agencies built relationships and documented how the state would deal with overwhelmed local response capability.

In 2019, DIR received funding from the Legislature to train applications developers in secure coding practices. DIR worked with the vendor partner to review and add appropriate courses to the existing course catalog such as Java and .net codes, along with two SecDevOps courses.

2019 – 86th Texas Legislative Session

SB 64 – SB 64 added the Prioritized Cybersecurity and Legacy Systems (PCLS) Report to the Government Code that was previously a rider in the General Appropriations Act. SB 64 expanded on HB 8 (2017) requirements regarding state agency reporting of certain security incidents to DIR, in addition to requiring DIR to identify and develop strategies to incentivize institutions of higher education to develop programs in cybersecurity by September 2020.¹⁹⁶ SB 64 required DIR to include in its biennial cybersecurity report an evaluation of a program to provide Information Security Officers to small agencies and local governments that could not justify hiring an Information Security Officer. Furthermore, it required public junior colleges and the Employees Retirement System to comply with information security standards established by DIR under Government Code Chapter 2054 and authorized public junior colleges to access Shared Technology Services (STS) programs. SB 64 also updated the requirement to establish an information sharing and analysis center, rebranding this center as an organization by which state agencies, local governments, public and private institutions of higher education, and the private sector could share cybersecurity information. SB 64 also authorized the State Cybersecurity Coordinator and Cybersecurity Council to develop cybersecurity best practices and establish the Cyberstar Certificate program. State agencies were granted authority to expend appropriated funds to reimburse certain employees for fees associated with industry-recognized certification examinations.

Implementation: In 2019, DIR formed the Texas Information Sharing and Analysis Organization (TX-ISAO) in partnership with the University of Texas at San Antonio and Texas A&M University. In June 2020, DIR began sharing intelligence with TX-ISAO members via email and conducting monthly TX-ISAO membership meetings. In August 2022, DIR implemented the TX-ISAO portal, which provides an efficient and secure method to share indicators of compromise (IOCs) and other actionable intelligence and information. Members may use the TX-ISAO to share best practices, lessons learned, and other insights.

DIR launched the Texas Cyberstar Certificate Program in May 2022.

¹⁹⁶ [Acts 2019, 86th Leg., R.S., ch. 509 \(S.B. 64\), 2019 Tex. Gen. Laws 1359 \(codified as an amendment to relevant sections of Government Code Chapter 2054\).](#)

[HB 3834](#) – HB 3834 directed DIR to annually certify at least five cybersecurity training programs for use by state and local governments and publish the list of certified cybersecurity training programs to the DIR website. It required state and local government employees, their elected and appointed officers, and state government contractors to complete an annual cybersecurity training and for organizations to report compliance annually. HB 3834 allowed local governments with a dedicated Information Resources Cybersecurity Officer to certify their own training program.¹⁹⁷

Implementation: During the initial implementation in 2019, DIR developed an exception form for local governments to report certifying their own training, and 95 local governments used that exception. DIR also worked with the Cybersecurity Council to identify 13 criteria to certify training programs. From September 2019 through April 2020, DIR certified 125 training programs. In May 2020, DIR developed and posted a video training program that received over 14,000 views on the agency’s website and YouTube channel.

The next year, DIR certified 146 training programs. Additionally, DIR posted on the agency’s website and YouTube channel the DIR-developed video training program in Spanish. Collectively, these English and Spanish videos received over 87,000 views. Also, 47 local governments used the exception allowing their dedicated Information Resources Cybersecurity Officer to certify their own training program. (In 2021, HB 1118 repealed this exception.)

The chart below reflects the cybersecurity programs DIR certified from FY19 to FY23.

Figure 44 Number of Training Programs DIR Certified

Fiscal Year	Number of Training Programs DIR Certified
FY19-20	125
FY20-21	146
FY21-22	160/Added spear phishing to training
FY22-23	122
FY23-24	TBD/Adding remote work practices

General Appropriations Act (2019) – Multi-factor Authentication (MFA) – DIR received authority from the 86th Legislature to implement a statewide MFA program for state agencies and institutions of higher education to provide a more uniform and secure authentication system by creating an extra layer of account security. DIR offers a MFA solution that provides basic identity and access management services to eligible customers at low to no cost.¹⁹⁸ According to the 2023 [Verizon Data Breach Investigations Report](#), 74 percent of security breaches are due to weak or stolen passwords that hackers can then use to access accounts. [Microsoft](#) reports that correctly using MFA can block over 99.9 percent of account compromise

¹⁹⁷ [Acts 2019, 86th Leg., R.S., ch. 1308 \(H.B. 3834\), 2019 Tex. Gen. Laws 3856 \(codified as an amendment to Government Code Chapter 2054\).](#)

¹⁹⁸ [General Appropriations Act, 86th, R.S., ch. 1353 \(H.B. 1\).](#)

attacks.

Implementation: DIR began offering MFA in October 2019. Today, DIR provides MFA to 10 direct customers in addition to providing MFA for large portals such as the Texas Comptroller of Public Accounts' Centralized Accounting and Payroll/Personnel System. Currently, nearly 75,000 users take advantage of the program, and another 31,200 users are in the process of being added.

2021 – 87th Texas Legislative Session

SB 475 – SB 475 authorized the creation of the Volunteer Incident Response Team (VIRT), the Texas Risk and Authorization Management Program (TX-RAMP), and Regional Security Operations Centers (RSOCs), all of which were recommendations included in DIR's [2020 Cybersecurity Report](#). Furthermore, the Legislature granted DIR additional general revenue funding and appropriations for full-time employees to support the Cybersecurity Incident Response Team (CIRT).¹⁹⁹

Implementation: Information on the implementation of SB 475's programs is below.

TX-RAMP – In December 2021, DIR adopted [1 Texas Administrative Code Chapter 202](#), the rules that administered the TX-RAMP Program, and published the TX-RAMP Program Manual to define the processes, procedures, and compliance requirements relating to the use of cloud computing services by Texas state agencies and institutions of higher education.²⁰⁰

RSOCs – In December 2021, DIR posted the RSOC Expression of Interest Overview, inviting all interested public institutions of higher education to submit proposals explaining why their institutions should be selected as the pilot RSOC. In April 2022, DIR selected Angelo State University to host the pilot RSOC; by July 2022, all necessary agreements and contracts were finalized. From July to December 2022, DIR and Angelo State University collaborated to establish the pilot RSOC. During this time, DIR granted Angelo State University flexibility in acquiring—or utilizing existing—technology solutions that made sense for their security operations.

VIRT – The 2019 ransomware attack made clear that should a substantial cyberattack occur, state resources would be stretched thin to adequately address the requirements of impacted entities. Following the model used in Michigan to develop a deeper bench of professionals to rely upon should a cybersecurity incident demand it, DIR developed and launched the Texas VIRT in December 2021 as an on-demand resource for significant cybersecurity incidents. The VIRT is composed of volunteers who meet DIR's requirements for selected volunteers – including a criminal background check – and have technical expertise in incident response,

¹⁹⁹ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\), § 6 \(codified at Government Code Chapter 2054, Subchapter N-2\).](#)

²⁰⁰ [1 Tex. Admin. Code Chapter 202.](#)

forensics, recovery, and remediation. A senior Cybersecurity Analyst in the CIRT manages the VIRT, which includes the maintenance of the VIRT Program handbook and creation of promotional content to recruit talented members. The VIRT reached a significant membership milestone in the Spring of 2023 when its membership exceeded 100 volunteers. Michigan runs a similar volunteer team that began in 2013 and counts 72 members.

General Appropriations Act (2021) – Endpoint Detection and Response (EDR) – In the 87th Legislative Session, DIR was appropriated approximately \$22 million in General Revenue for EDR technology in a new initiative to help provide those services to state agencies and institutions of higher education at little to no cost to them.²⁰¹ This initiative protects state-issued computers, laptops, servers, and other endpoints from ransomware and other threats. Because DIR procured the tool through DIR’s contracts, DIR can offer EDR at a reduced cost for the state, and even local governments can take advantage of the highly reduced costs through the tiered pricing models included in the DIR contracts.

Implementation: DIR began providing EDR through the Managed Security Services (MSS) program in September 2021 and, as of June 2023, the program is protecting more than 119,000 computing devices.

SB 1696 – SB 1696 directed the Texas Education Agency to collaborate with DIR to establish and maintain a system to coordinate sharing information about school district cybersecurity incidents statewide with the state.²⁰²

Implementation: In September 2021, DIR updated the Texas Information Sharing and Analysis Organization (TX-ISAO) threat report to include school district incident reporting. The associated intelligence is shared with other schools through the TX-ISAO Portal.

HB 1118 – HB 1118 updated the annual cybersecurity training requirements for local governments and school districts, removed the exception allowing local governments to certify their own training program, and directed DIR to develop a form for state and local governments to report training completion.²⁰³ Additionally, HB 1118 required state and local governments to include a certification of training compliance in the state agency strategic plan and certain grant applications.

Implementation: DIR updated the cybersecurity training webpage with the revised training requirements for state and local governments. DIR removed the exception form for local governments to report certifying their own training and contacted entities that had previously reported this exception. DIR also updated the training compliance form to include a statement of training compliance that could be included with state agency strategic plans and grant

²⁰¹ [General Appropriations Act, 86th, R.S., ch. 1353 \(H.B. 1\).](#)

²⁰² [Acts 2021, 87th Leg., R.S., ch. 618 \(S.B. 1696\), § 2 \(codified as an amendment to Educ. Code § 11.175\).](#)

²⁰³ [Acts 2019, 86th Leg., R.S., ch. 1308 \(H.B. 3834\), 2019 Tex. Gen. Laws 3856 \(codified as an amendment to Government Code Chapter 2054\).](#)

applications.

DIR worked with the Office of the Governor to develop a process where grant staff could verify local governments' training compliance. Initially, the Governor's Office provided a list of grant applicants to DIR to verify. In March 2022, DIR implemented a system for Office of the Governor Grant Managers to verify training compliance directly.

Cybersecurity legislation passed in the 88th Legislative Session is discussed in VIII. Statutory Authority and Recent Legislation.

Significant Cybersecurity Incidents

This section details significant cybersecurity incidents that required DIR's response, including the 2019 ransomware event impacting 23 local governments, ransomware incidents at three state agencies, and several security vulnerabilities.

2019 Ransomware Incident

On August 16, 2019, at 8:36 a.m., DIR received notification that eight local governments had been attacked with suspected Sodinokibi ransomware. By 11:00 a.m., the number of impacted entities had grown to 19. After notifications and discussions with DIR, Governor Abbott issued the State of Texas' first statewide disaster declaration for a cybersecurity incident. With the Governor's disaster declaration, the Cybersecurity Annex to the Texas Emergency Management Plan was put into action. The disaster declaration also activated the Texas Division of Emergency Management's (TDEM) State Operations Center (SOC) to Level Two, which approves 24-hour, seven-days-a week operations. By noon, the SOC was fully active with DIR leading the response, and multiple state and federal incident responders reporting to the SOC.

Ultimately, the incident impacted 23 Texas government entities and approximately 740 computers. All of the entities shared a private managed services provider and the attacker used the provider's server to remotely execute the ransomware on the entities' workstations and servers.

By noon the following day, Saturday, August 17, 2019, Texas incident responders had identified and prioritized all impacted entities. By the end of Sunday, August 18, 2019, incident responders had made in-person visits to all impacted entities across Texas. By the end of Friday, August 23, 2019, one week after the incident began, all impacted entities had been remediated to the point that state support was no longer required.

Per the State of Texas Cybersecurity Annex, DIR led the incident response effort. Other state responders included: the Texas Military Department, Texas Division of Emergency Management, Texas A&M University System's Security Operations Center/Critical Incident Response Team, Texas Department of Public Safety, Public Utility Commission of Texas, Texas Water Development Board, Texas Commission on Environmental Quality, and private sector vendors. Federal responders included: the Federal Bureau of Investigation, the Department of Homeland Security, and the Federal Emergency Management Agency.

Though the cyber attackers set the ransom payment at \$2.5 million, no ransom or portion of

the ransom was paid. In 2021, the U.S. Justice Department charged and extradited a Ukrainian national, charged a Russian national, and seized \$6.1 million in funds allegedly traced to ransomware payments; both individuals had ties to the ransomware group responsible for the cyberattack, which has been linked to a Russian-speaking, private ransomware threat actor.

This coordinated state and federal response to a statewide, multi-jurisdictional cybersecurity incident was later identified as the largest coordinated ransomware attack against local governments in the U.S. at the time. By successfully executing the statewide cybersecurity incident response plan, DIR and its state and federal partners ensured that all affected local government entities were operational in seven days—an unprecedented feat for the size of the attack. Because of the success of the Texas response and received international attention, DIR’s Executive Director was asked to testify in front of the U.S. Senate Homeland Security and Governmental Affairs Committee. The committee sought to learn from the successful Texas response, replicate it in other states, and inquire as to how the federal government could assist states more in this area.

State Agency Ransomware Incidents

As the cybersecurity agency for the state, DIR is responsible for providing security services to certain government entities to support their recovery from a security incident. Furthermore, many public sector entities are required by law to report security incidents to DIR. These entities trust DIR to protect the reported information, if applicable, as well as any information that DIR collects or otherwise accrues in its efforts to assist or support the agency in its recovery from the security incident. DIR considers any documentation or information in its possession regarding a security incident, either its own or another entity’s, to be confidential pursuant to Texas Government Code Section 552.139. DIR has anonymized the incidents described in this report to reflect its work with the entity to resolve the incident while still maintaining the anonymity of its customer to avoid inviting scrutiny by bad actor’s or otherwise further exposing the entity’s network security vulnerabilities.

Agency A²⁰⁴

On May 14, 2020, Agency A was severely impacted by Defray ransomware affecting critical application servers in the agency’s Austin and regional offices in addition to the agency’s systems within DIR’s Shared Technology Services (STS) Data Center Services.

Available evidence suggests that the cyber attackers used a contractor’s compromised account to gain access to Agency A’s network through a regional office. However, the attackers erased most system logs, making it difficult to determine the exact attack vector. The cyber attackers encrypted 76 servers supporting multiple business-critical applications.

²⁰⁴ For security purposes, the names of the impacted agencies can be submitted separately to the Sunset Advisory Commission upon request.

Agency A uses DIR's Data Center Services. As such, DIR supported the immediate response and incident investigation and was responsible for the recovery of the impacted servers. DIR provided two Cybersecurity Analysts (one DIR employee and one contractor) that worked every shift of the STS' Security Incident Response Team's communications bridge, which operated continuously for 24 days. DIR provided protection for Agency A while they were vulnerable, supporting the Security Incident Response Team investigation, mitigation, and critical applications recovery efforts.

To recover the servers, analysts used unimpacted backups from the data center. The recovery operation lasted a total of 102 days and required 1,152 DIR staff hours dedicated entirely to its response.

In addition to staffing resources, DIR provided Agency A access to Microsoft's Unified Support contract (to support incident response and recovery activities) and DIR's Managed Security Services (to support the onsite incident investigation).

Furthermore, DIR funded advanced threat hunting capabilities to search for any indications of cyber attackers infiltrating other state agencies. No evidence of infiltration was found in the other state agencies.

Agency B

On May 8, 2020, a suspected phishing incident at Agency B resulted in the NetWalker ransomware encrypting Agency B's email system and files hosted on the Agency B network.

Compromised by a suspected phishing attack, this incident impacted Agency B's operational systems and limited its ability to process and manage workloads, send emails, and access encrypted data. The cyberattack interrupted business operations at numerous connected entities (including local entities), delaying government processes in Texas.

DIR provided over 300 staff hours of onsite support, including a Deputy Chief Information Security Officer and multiple Cybersecurity Analysts. DIR provided access to Microsoft's Unified Support contract to support incident response and recovery activities, and DIR's Managed Security Services ensure that the malicious actors were completely expelled from Agency B systems in addition to hunting for other threats in the environment.

Within three weeks, Agency B could resume some business operations; after six weeks, Agency B completed the rebuild, which resulted in their hardening of their infrastructure. Agency B did not engage with the cyber attackers or pay the ransom, which was close to one million dollars demanded in cryptocurrency.

Agency C

On April 26, 2021, Agency C was impacted by the Avaddon ransomware encrypting all files and devices connected to its network.

This cybersecurity incident impacted Agency C's ability to process licensing requests and other business-critical activities. Agency C lacked the technical and forensic capabilities to adequately

determine the cause of the incident.

After Agency C notified DIR of the ransomware, DIR provided incident containment guidance including forensics guides to support Agency C's investigation; performed network analysis activities to help Agency C determine the source of the initial compromise; ordered, funded, and guided forensics to help determine the extent of the compromise and provide guidance on recovery; and supported executive communication between Agency C and other involved government entities.

Security Vulnerabilities

A security vulnerability is a weakness, flaw, or error (such as a software coding deficiency or system misconfiguration) that threat actors can exploit to gain unauthorized access to a system. Since 2020, several vulnerabilities have emerged on services used by government entities that involved a response from DIR. Those security vulnerabilities are detailed below.

SUNBURST (SolarWinds) Vulnerability

SUNBURST was the first major supply chain cyberattack targeting SolarWinds' Orion software, a network monitoring application with a major market share, leading to breaches in multiple organizations including government agencies.

The cyber attackers infiltrated the SolarWinds Orion platform and injected it with malware, which is now known as SUNBURST. As users upgraded their SolarWinds products to the latest versions, they also unknowingly installed the SUNBURST malware that provided the threat actors with backdoor access to the users' networks. On December 8, 2020, the security company FireEye discovered SUNBURST when they found the malware in their network after investigating their own security breach.

Log4j Vulnerability

The Log4j vulnerability (also known as Log4Shell) affected the Apache Log4j logging library, which is widely used in various Java-based applications. This vulnerability emerged in December 2021, providing an opening for threat actors to inject malicious code into the logs that could be executed on a system.

Microsoft Exchange Zero-Day Vulnerability

In March 2021, the HAFNIUM advanced persistent threat group targeted Microsoft's on-premises exchange server exploiting a total of four zero-day vulnerabilities. These vulnerabilities allowed unauthorized threat actors to compromise Microsoft Exchange Servers to gain an unauthorized foothold into a system, and access server files and mailboxes.

Microsoft Print Nightmare Vulnerability

In June 2021, a security researcher discovered a critical vulnerability affecting the print spooler system of the Microsoft Windows operating system that could lead to both remote code execution and privilege escalation. Microsoft released multiple unscheduled patches to address these vulnerabilities.

MOVEit Vulnerability

MOVEit is a popular data transfer application used by organizations to move large datasets across the internet. The CL0P ransomware group exploited a previously unknown vulnerability in the application that allowed access to the datasets being transferred. The CL0P ransomware group used this vulnerability to exfiltrate large amounts of data from government and commercial organizations.

On May 31, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) announced the CL0P ransomware group activities as an exploited zero-day vulnerability.

DIR's Response

DIR conducted the following activities for all the vulnerabilities listed above:

- Identified indicators of compromise (IOCs) and added the IOCs to the Network Security Operations Center (NSOC) toolsets for blocking and detection, including custom alerts and dashboards specific to the threat; alerted agencies to any activity detected.
- Investigated network traffic logs for any previous connections made to and from the threat actors and alerted the affected agencies.
- Coordinated scans for IOCs and the presence of the vulnerable hardware and software in the state's shared data centers, and alerted agencies of the critical vulnerability in their environment.
- Supported and assisted affected agencies with their response and mitigations.
- Published statewide notifications on the vulnerability to provide guidance and advice to DIR customers.
- Hosted conference calls with statewide organizations to provide situational awareness.
- Offered and provided remediation and eradication efforts to local government entities.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The following entities are eligible for services DIR provides, including programs within the

Cybersecurity function:²⁰⁵

- State agencies;
- Local government organizations;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Texas Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Texas Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Texas Tax Code Section 152.001; and
- Government entities of another state.

DIR's Cybersecurity function ultimately impacts every Texan who interacts with state and local government as DIR oversees and manages the protection of the state's data and infrastructure and assists local governments through services and programs.

Figure 45 Eligibility Requirements for DIR Services

DIR Service	Eligibility Requirements
DIR-funded security services such as Managed Security Services (MSS), Multi-Factor Authentication (MFA) program, InfoSec Academy offerings, research and advisory services, and end user security awareness training services	• State agencies • Institutions of higher education • Public junior colleges
Cybersecurity Incidence Response Support through the Cybersecurity Incident Response Team (CIRT)	• State agencies • Political subdivisions, including counties or municipalities • K-12 school districts and open enrollment charter schools • Institutions of higher education • Public junior colleges

²⁰⁵ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

DIR Service	Eligibility Requirements
Regional Security Operations Center (RSOC) Cybersecurity Services	· State agencies · Political subdivisions, including counties and municipalities · Independent organizations as defined by Texas Utilities Code § 39.151 · Each house of the Legislature · Public junior colleges · Independent organizations as defined by Utilities Code Section 39.151(b) · Special districts, defined as school districts, hospital districts, water districts, or districts or special water authorities as defined by Texas Water Code § 49.001 · Agencies that are not state agencies, including a legislative agency
Texas Information Sharing and Analysis Organization (TX-ISAO)	· Any Texas entity, including private sector organizations
Texas Cyberstar Certificate	· Public and private entities
Information Security Forum	· Public entities
Educational Webinars	· Everyone
Regional Working Groups	· State agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the Volunteer Incident Response Team (VIRT) ○ A working group may be established within the geographic area of a regional planning commission established under Texas Government Code Chapter 391.122. The working group may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity incident and recovery from the incident.
Volunteer Incident Response Team (VIRT) Volunteer Eligibility	· Expertise in addressing cybersecurity incidents including knowledge, skills, and abilities in cybersecurity incident response; · Ability to successfully complete a background check, which is subject to periodic re-verification; · Agree to sign a contract with DIR, which outlines; · Volunteer information confidentiality and non-disclosure; · Requirements to avoid conflicts of interest during a deployment; · Other specifications relevant to the operation of the VIRT; and · Ability to travel to an incident site or operations center on short notice for a defined period of time or to provide remote support, as appropriate.

- f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.**

Cybersecurity Administration

Protecting the state from cyber threats is DIR's top priority, and therefore, nearly every division in the agency touches the Cybersecurity function. DIR has dedicated two divisions and five teams to the Cybersecurity function because it is such a multi-faceted and complex topic. The DIR divisions with primary responsibility for the Cybersecurity function are the Chief Operations Office (COO) and the Office of the Chief Information Security Officer (OCISO).

The Cybersecurity Operations team is part of the Chief Operations Office, and OCISO contains four teams: the Policy and Governance team, the Cybersecurity Coordination team, the Security Operations/Cybersecurity Incident Response Team (CIRT), and the Security Services team.

In total, DIR has approximately 34 current full-time employees working with a number of contractors dedicated to accomplishing the many programs and services DIR provides under the Cybersecurity function.

Though tasked with different responsibilities, the COO and OCISO work closely together and coordinate often, specifically when responding to cybersecurity incidents at state agencies.

Cybersecurity Operations Team

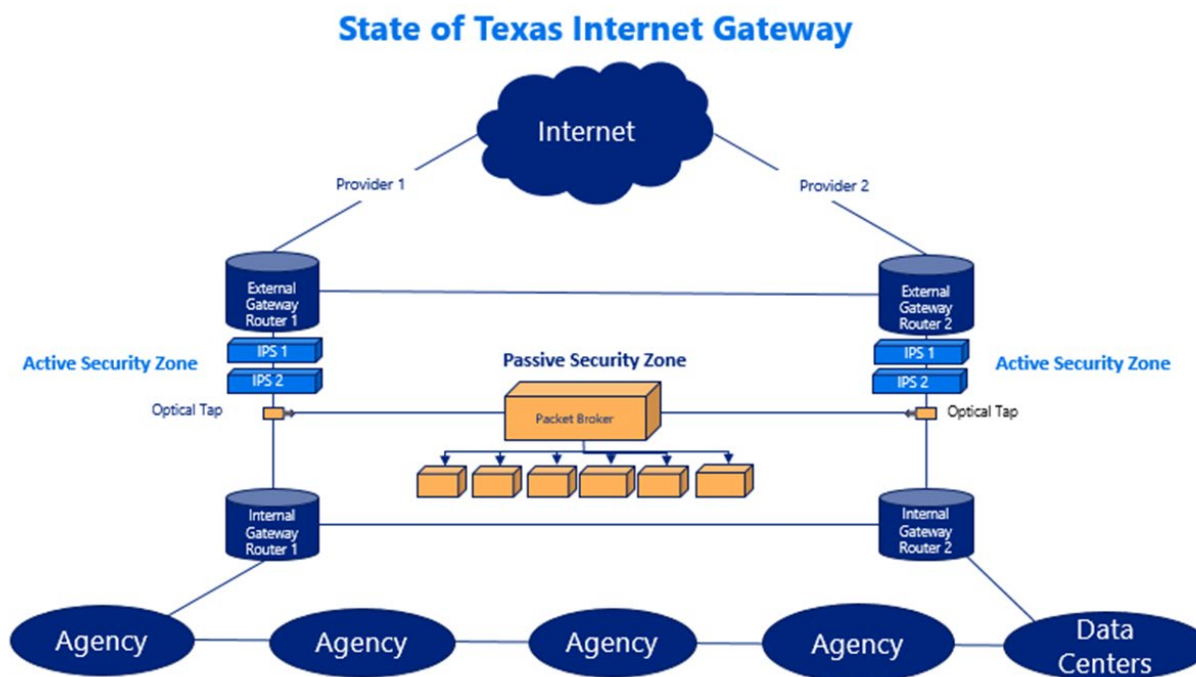
The Cybersecurity Operations team is administered by the Director of Cybersecurity Operations, who reports to DIR's Chief Operations Officer. The Cybersecurity Operations team includes a DIR Cybersecurity Operations Team Lead and six DIR Cybersecurity Analysts overseeing a staff of 23 contracted Cybersecurity Analysts to support 24-hour, seven-days-a week operations.

The Cybersecurity Operations team manages the network security system services for all state agencies at the Network Security Operations Center (NSOC). The NSOC serves as the headquarters for the State of Texas' network security services and maintains real-time network security monitoring to detect and respond to network security events.

The Cybersecurity Operations team manages the development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and mitigate the impact of network security incidents. To accomplish these responsibilities, DIR implements best-of-breed cybersecurity technologies and services, including blocking unwanted or threatening network traffic, alerting agencies to suspicious traffic, detecting and mitigating distributed denial-of-service (DDoS) attacks, and network security forensics.

The chart below illustrates the NSOC's architecture.

Figure 46 DIR Internet Gateway Architecture



The Cybersecurity Operations team is responsible for the oversight of cybersecurity operations in the Shared Technology Services (STS) program. The team provides guidance to vendors providing new security technologies and tools as well as creating and maintaining policies, processes, and procedures for Data Center Services (DCS). The team responds to all major security incidents in DCS and provides guidance and investigative support to customers connected to the DIR network.

In addition to managing the NSOC, the Cybersecurity Operations team provides threat intelligence reports based on observations while monitoring Texas' network. These threat intelligence reports are shared with OCISO and other state agencies, including the Office of the Governor.

The Cybersecurity Operations team also oversees phishing email analysis. DIR invested in tools that provide analysts the ability to perform deep analysis of suspicious emails safely and securely. Agencies submit suspicious emails to the NSOC, after which the Cybersecurity Operations team analyzes the email and collects any indicators of compromise (IOCs), which are IP addresses, domain names, URLs, and file hashes. These IOCs are then added to the NSOC toolsets for blocking and alerting purposes. The team creates and shares a weekly report of these IOCs with the Texas Information Sharing and Analysis Organization (TX-ISAO) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

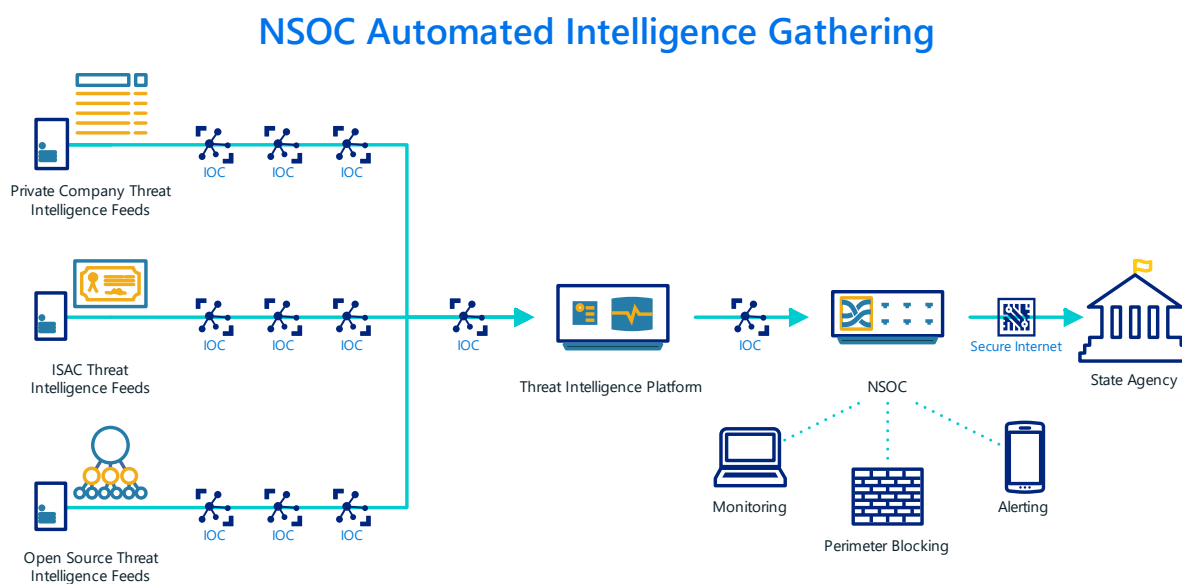
The Cybersecurity Operations team oversees the daily operations of the state-funded Managed Security Services (MSS) Endpoint Detection and Response (EDR) program. This program provides endpoint protection and active response via an agent installed on the endpoint. To date, that program is monitoring and protecting over 100,000 computing devices. All the data

collected through these endpoints is available to the Cybersecurity Operations team.

Comprehensive, timely threat intelligence is key to effective network security. The DIR Cybersecurity Operations team uses a threat intelligence platform that automatically shares new threat intelligence with other security entities. By making use of both open-source intelligence and exclusive fee-based intelligence feeds, DIR adds an average of 5,000 new IOCs (out of 100,000 new IOCs that are available via the feeds) every day.

The following graphic illustrates this process.

Figure 47 NSOC Automated Intelligence Gathering



Office of the Chief Information Security Officer

The Office of the Chief Information Security Officer (OCISO) includes approximately 26 current full-time employees and is led by the Chief Information Security Officer, who directs four Deputy CISOs. Each Deputy Chief Information Security Officer (or Deputy CISO) heads one of the following teams: Cybersecurity Coordination, Policy and Governance, Security Operations/Cybersecurity Incident Response Team (CIRT), and Security Services. While each team oversees specific responsibilities and programs, the division shares responsibility for answering the security incident hotline, monitored around-the-clock, and responding to inquiries regarding cybersecurity.

The four teams and programs are reflected in the chart below.

Figure 48 Four Teams within the Office of the Chief Information Officer

Policy and Governance	Security Operations	Security Services	Cybersecurity Coordination
· TAC 202 and Security Controls Catalog · Texas Cybersecurity Framework · Texas Risk and Authorization Management Program (TX-RAMP) · Security Planning and Reporting · Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM)	· Volunteer Incident Response Team (VIRT) · Cybersecurity Incident Response Team (CIRT) · Regional Security Operations Center (RSOC) · Statewide Incident Response Coordination	· Security Training · Assessments and Pen Tests · Information Security Forum (ISF) · Shared Technology Services Security · Multi-factor authentication (MFA)	· Texas Information Sharing and Analysis Organization (TX-ISAO) and Threat Reporting · Public and Private Sector Collaboration · Statewide Security Awareness Training · Texas Cybersecurity Council

Policy and Governance Team

The Policy and Governance team implements statutorily required information security initiatives, collects information about the security posture of government entities, and develops recommendations for improving the security of government entities.

The Policy and Governance team focuses on improving the security posture of government entities by setting minimum security standards, assessing cloud computing service providers for Texas Risk and Authorization Management Program (TX-RAMP) certification, maintaining the Texas Cybersecurity Framework (TCF), and providing tools and services through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) for agencies to mature their information security programs.

The Deputy Chief Information Security Officer for Policy and Governance administers this team, which includes seven DIR Cybersecurity Analysts. In addition to this team of DIR employees, the Deputy Chief Information Security Officer also oversees three contractors and one Professional Services Consultant to develop and oversee statewide governance, risk, and compliance matters. The team provides support to agencies and universities through the statewide governance, risk, and compliance platform offerings, collects agency information, produces legislative reports, and administers TX-RAMP.

DIR manages the related Texas Administrative Code rules²⁰⁶ and TX-RAMP Program Manual, which defines the specific processes, procedures, and security control criteria to obtain a

²⁰⁶ 1 Tex. Admin. Code §§ [202.27](#), [202.77](#).

certification.

The Cybersecurity Analysts assist with designing the workflows, notifications, reports, processes, and documentation of team functions. Additionally, the team provides technical support, troubleshooting, user administration, communications, and guidance to stakeholders in addition to performing security control assessments of cloud computing services for TX-RAMP certification.

The contractors provide TX-RAMP assessment assistance, leveraging highly technical knowledge and experience.

The Professional Services Consultant provides expertise, design, and development services related to SPECTRIM.

Security Operations/Cybersecurity Incident Response Team (CIRT)

The Security Operations/CIRT team, referred to as the CIRT, aims to safeguard the state's critical assets by offering incident response support and sharing threat intelligence to eligible organizations. The CIRT provides cybersecurity incident response support, oversees the Volunteer Incident Response Team (VIRT) and Regional Security Operations Center (RSOC) programs, prepares statewide incident response plans, and helps other entities plan and train for cyberattacks.

Following the passage of [Senate Bill 475](#), DIR established the CIRT in November 2021 to implement the pilot RSOC and the VIRT, and focus on incident response efforts.²⁰⁷ Since then, the CIRT has helped mitigate 40 ransomware incidents, including three onsite deployments.

The Deputy Chief Information Security Officer for Security Operations/CIRT administers this team and is responsible for overseeing incident response to Texas entities, the RSOC, and the VIRT. The team is composed of the Statewide Incident Response Coordinator, a Cybersecurity Analyst Team Lead, three Cybersecurity Analysts, two Threat Research Analysts, and a Program Specialist.

The Program Specialist is responsible for the team's travel, maintaining metrics and tracking, and developing and maintaining local government IT contact information. If the CIRT is approved for onsite deployment, the Program Specialist coordinates urgent requests regarding travel authorizations, including travel request forms, hotel reservations, and transportation resources.

The Technical Writer, who is under the Deputy Executive Director, standardizes all communication from the CIRT and is primarily responsible for writing and editing reports, briefs, plans, incident documentation, guides, presentations, bulletins, advisories, and all other

²⁰⁷ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\)\(codified as an amendment to relevant sections of Texas Government Code Chapter 2054\).](#)

official communications from the CIRT.

Along with responding to an event when DIR is notified, the CIRT proactively searches for information about Texas entities to notify them of compromises. The CIRT's Threat Research Analysts are responsible for searching the dark and deep web for Texas cities, counties, and other public entities that may have cybersecurity issues exposed. The CIRT gathers cybersecurity intelligence from a variety of sources including cybersecurity incidents, threat intelligence feeds, threat research of the dark and deep web, coordination with other state agencies, and trusted third-party cybersecurity advisories. Threat intelligence includes common misconfigurations, vulnerabilities that do not align with cyber hygiene best practices, and vulnerabilities being actively targeted by cyber threat actors. Additionally, the Threat Researchers search for other cybersecurity intelligence including information such as the tactics, techniques, and procedures that threat actors use to execute cyberattacks and known indicators of compromise (IOCs) that IT professionals can use to detect intrusion attempts and other malicious activity. The threat researchers cross-check the threat information with the Cybersecurity and Infrastructure Security Agency's (CISA) information to make sure vulnerabilities are correctly addressed. The threat researchers notify the entities of vulnerabilities found that are impacting—or may impact—the entity.

After gathering cybersecurity intelligence, the CIRT distributes the cybersecurity intelligence via forensic analysis reports, white papers, cybersecurity bulletins, vulnerability notifications, presentations, and intelligence briefings.

A Cybersecurity Analyst is responsible for distributing the information via the TX-ISAO. Recipients of this cybersecurity intelligence can then use it to inform their own cybersecurity operations.

DIR is a member of the Texas Homeland Security Council, which develops the Texas Homeland Security Strategic Plan and tasks all supporting agencies with helping achieve Texas' long-term homeland security goals. Specifically, DIR contributes to the development of the Texas Homeland Security Strategic Plan by tracking the plan's implementation metrics, developing the plan with other participating agencies, and participating in meetings and task forces regarding the plan. DIR is tasked with helping Texas achieve several cybersecurity priority actions outlined in the most recent plan.

In support of this multi-year strategic plan, the Statewide Incident Response Coordinator develops a yearly agency implementation plan to guide DIR's efforts in meeting Texas' homeland security objectives and aligning agency priorities to Texas' homeland security goals.

Developing the agency implementation plan involves coordinating with other state agencies to focus Texas' cybersecurity efforts, resolving currently outlined known issues, and anticipating and planning for the future of cybersecurity. The plan is developed through several rounds of drafting, reviewing, and editing before being published each December.

DIR is also a member of the Texas Emergency Management Council and is responsible for the Emergency Support Function (ESF)-20 Cybersecurity Annex to the State of Texas Emergency

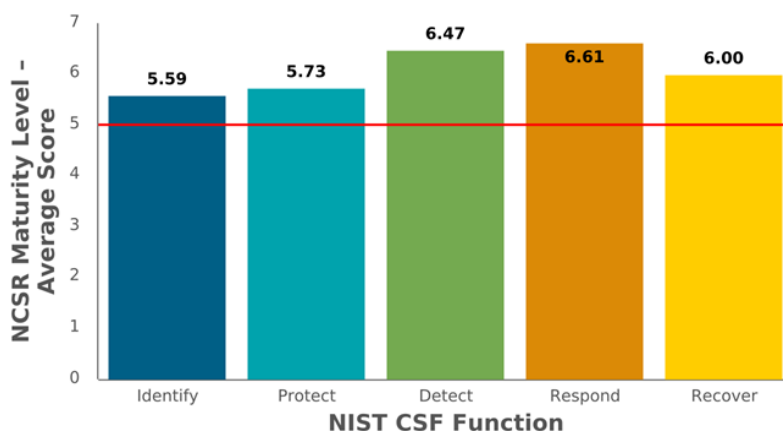
Management Plan, which is being developed in cooperation with members of the Statewide Incident Response Workgroup, the Texas Division of Emergency Management Preparedness Team, and the Texas Emergency Management Council. To develop the ESF-20 Cybersecurity Annex, the Statewide Incident Response Coordinator regularly meets with the entities to develop procedures for achieving each objective of the annex, including information on identified processes, staff, and tools.

The Statewide Incident Response Coordinator works with the Statewide Incident Response Workgroup to develop and maintain the Statewide Cyber Incident Response Plan, which addresses cybersecurity risks and incidents in the state, in alignment with [Government Code Section 2054.518](#).²⁰⁸

Additionally, the Statewide Incident Response Coordinator completes the annual Nationwide Cybersecurity Review (NCSR), a self-assessment of the state's level of cybersecurity maturity as assessed against the National Institute of Standards and Technology (NIST) Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. To develop an accurate assessment of the state's cybersecurity maturity, the NCSR asks questions about activities performed in each of the functions and associated framework categories. The Statewide Incident Response Coordinator reviews the results of assessments, security plans, and other governance and risk management documents to develop an accurate understanding of cybersecurity maturity.

The chart below provides an overview of the 2022 NCSR self-assessment results.

Figure 49 DIR's 2022 NCSR Self-Assessment Results



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

The Security Operations/CIRT team helps entities test their unique incident response plans. The role of the CIRT Team Lead is to develop and facilitate tabletop exercises to eligible entities upon request, often with the support of a Cybersecurity Analyst. The content of these tabletop

²⁰⁸ [Gov't Code § 2054.518](#).

exercises is customized depending on the entity and its needs. These tabletop exercises include a scenario to prompt discussion and have the entity consider what its response would be in a hypothetical cybersecurity incident. Tabletop exercises proactively prepare an entity's incident response protocols before becoming necessary by having the entity consider how they would handle the situation in a safe, controlled environment.

Members of the CIRT regularly present at outreach events such as membership organization meetings or the annual DIR Information Security Forum (ISF) conference. At these events, the CIRT acts as a technical resource, providing guidance on cybersecurity incident response and planning or facilitating tabletop exercises. The team has presented at notable events such as the Texas Association of County's Annual Information Technology Conference, Texas Association of Government Information Technology Managers Annual Conference, Texas Association of State Systems for Computing and Communications conferences, and the 2023 Texas Digital Government Summit.

Security Services Team

The Security Services team provides and manages security services for the state to ensure that customers feel empowered, protected, and informed to comply with state information security policies and standards. DIR encourages its customers to obtain professional training and education, incident response support, and managed services to improve security resilience for the state. The Security Services team provides DIR-funded services to over 200 organizations and educational opportunities to all Texas public sector entities.

The Security Services team works closely with the Shared Technology Services (STS) program in DIR's Chief Operations Office and is administered by a Deputy Chief Information Security Officer, who oversees the Statewide Security Services Manager, the STS Information Security Officer, the Multi-factor Authentication (MFA) Program Manager, and the MFA Program Project Manager.

The STS Information Security Officer, along with the Cybersecurity Operations team, oversees the security of the STS programs. The STS Information Security Officer is responsible for ensuring appropriate security is applied throughout the program in documentation, practices, and processes, which is achieved through attending and participating in governance meetings, reviewing program documentation, informing DIR's customers of their risks, supporting incident response, assisting in audits, and meeting with DIR's customers. The STS Information Security Officer oversees the cybersecurity risk letters informing state agency Executive Directors of critical- and high-caliber cybersecurity risks existing on the agencies' systems in the state data center that may require additional resources, both time and financial, from those agencies to mitigate and remediate.

The MFA Program Manager and the MFA Project Manager work with current and potential customers to help them determine if DIR's MFA offering is a suitable option for a customer's use case. Throughout the life of projects, the MFA Program Manager acts as a liaison between the vendor provider and the customer to ensure a consistent and dependable experience for the customer. DIR works with the vendor to continue to develop and evolve the solution to

account for changing technologies and security practices.

The Statewide Security Services Manager coordinates the composition and framework for the DIR-funded penetration tests and risk assessment services with the vendor, acts as a liaison to existing and new customers, participates in customer engagement meetings, and handles escalations as necessary. DIR funds penetration testing and vulnerability assessments for state agencies, institutions of higher education, and public junior colleges. Penetration tests identify weaknesses in system configurations and network infrastructure that may lead to data breaches or malicious attacks. The penetration testing findings result in recommendations to amend systems configurations and security protocols to overcome security gaps. Security assessments are based on the Texas Cybersecurity Framework (TCF) and ensure alignment with cybersecurity best practices and controls. The assessments include recommendations and action plans to improve the entity's cybersecurity posture. These DIR-funded services are provided through STS by the contracted Managed Security Services (MSS) provider. The Statewide Security Services Manager role also organizes, plans, and runs monthly security meetings as well as plans and executes the Information Security Forum (ISF) in coordination with the Education and Outreach staff in DIR's Chief Experience Office. The ISF is an annual educational conference that brings together security and IT professionals from public sector organizations across Texas. Additionally, the Statewide Security Services Manager oversees the DIR-funded security awareness training and phishing simulation exercises offered to state agencies. This role also manages the InfoSec Academy, which provides top-tier training and funds certification exam vouchers for security, data management, and data science professionals employed at state agencies, institutions of higher education, and public junior colleges. DIR contracts with a third-party to provide these services and has developed guidelines and processes surrounding the program's requirements.

Cybersecurity Coordination Team

The Cybersecurity Coordination team provides cybersecurity support and resources to local government entities.

The Cybersecurity Coordination team focuses on improving the security posture of Texas entities, with a focus on local government entities, by administering the TX-ISAO portal to provide a forum for collaboration and intelligence sharing, setting certification standards for security awareness training programs, assessing the programs, leading the Texas Cybersecurity Council, and providing technical and educational opportunities through the TX-ISAO for Texas entities to mature their information security programs.

The Cybersecurity Coordination team provides support to all Texas entities through the statewide TX-ISAO platform offerings, collects local government information, develops legislative recommendations under the Texas Cybersecurity Council, and administers the Texas Cyberstar Certificate Program. Additionally, the team provides technical support, troubleshooting, user administration, communications, and guidance to stakeholders as well as performing security awareness training program assessments.

The Cybersecurity Coordination team is administered by the Deputy Chief Information Security

Officer who is also the State Cybersecurity Coordinator. The Cybersecurity Coordination team includes a Program Manager and a Cybersecurity Analyst to develop and oversee statewide security initiatives.

The Program Manager plans, evaluates, coordinates, drives, and supports the development, implementation and maintenance of initiatives and partnerships to promote the state's cybersecurity efforts.

The Cybersecurity Analyst processes TX-ISAO membership requests, performs security awareness training program assessments, processes Texas Cyberstar Certificate requests, and assists with designing the workflows, notifications, reports, processes, and documentation of team functions.

Cybersecurity Processes

Cybersecurity Operations Detection and Response Processes

Since the main mission of the Cybersecurity Operations team at the NSOC is to detect, triage, and alert agencies of security events, the team uses this same expertise to provide oversight of the incident handling process when DIR management deems it necessary or appropriate. When a cybersecurity incident occurs at a state agency, the level of Cybersecurity Operations oversight depends on the incident declarations below.

- **NSOC Incidents:** Incidents impacting the network, which may include network attacks, equipment failures, or critical infrastructure outages. For all NSOC-declared security incidents, DIR will manage the incident from detection to recovery. Often, DIR NSOC incidents can affect multiple customers. When multiple agencies/customers are impacted, immediate notification will be provided to DIR operations management.
- **Shared Services Incidents:** Incidents within the Shared Technology Services (STS) program where DIR is not the incident owner but is responsible for oversight of the service providers working the incident. For all shared services-declared incidents, the Multi-Sourcing Services Integrator (MSI) owns the security incident management processes and procedures. For these incidents, DIR provides oversight, including support, guidance, and analysis to the affected customers. DIR provides timely status reports of all shared services incidents to DIR management.
- **Agency Incident Declaration:** Incidents that occur solely within an agency that the agency owns and manages. The Cybersecurity Operations team provides any assistance and guidance to an agency requesting assistance but will not take ownership of the agency's incident. Normally, this involves investigating traffic, collecting packet captures, behavior analysis, and other DIR-collected information to support the impacted agency's remediation efforts.
- **Multi-Agency/Statewide Incident Declaration:** Incidents that, because of the scope or the nature of specific identified activities, require additional attention and action

as detailed by [1 Texas Administrative Code Chapter 202](#).²⁰⁹ For these incidents, DIR owns the security incident management processes and procedures. DIR management determines if the Cybersecurity Operations team or OSICO will lead incident response.

Texas Risk and Authorization Management Program (TX-RAMP) Processes

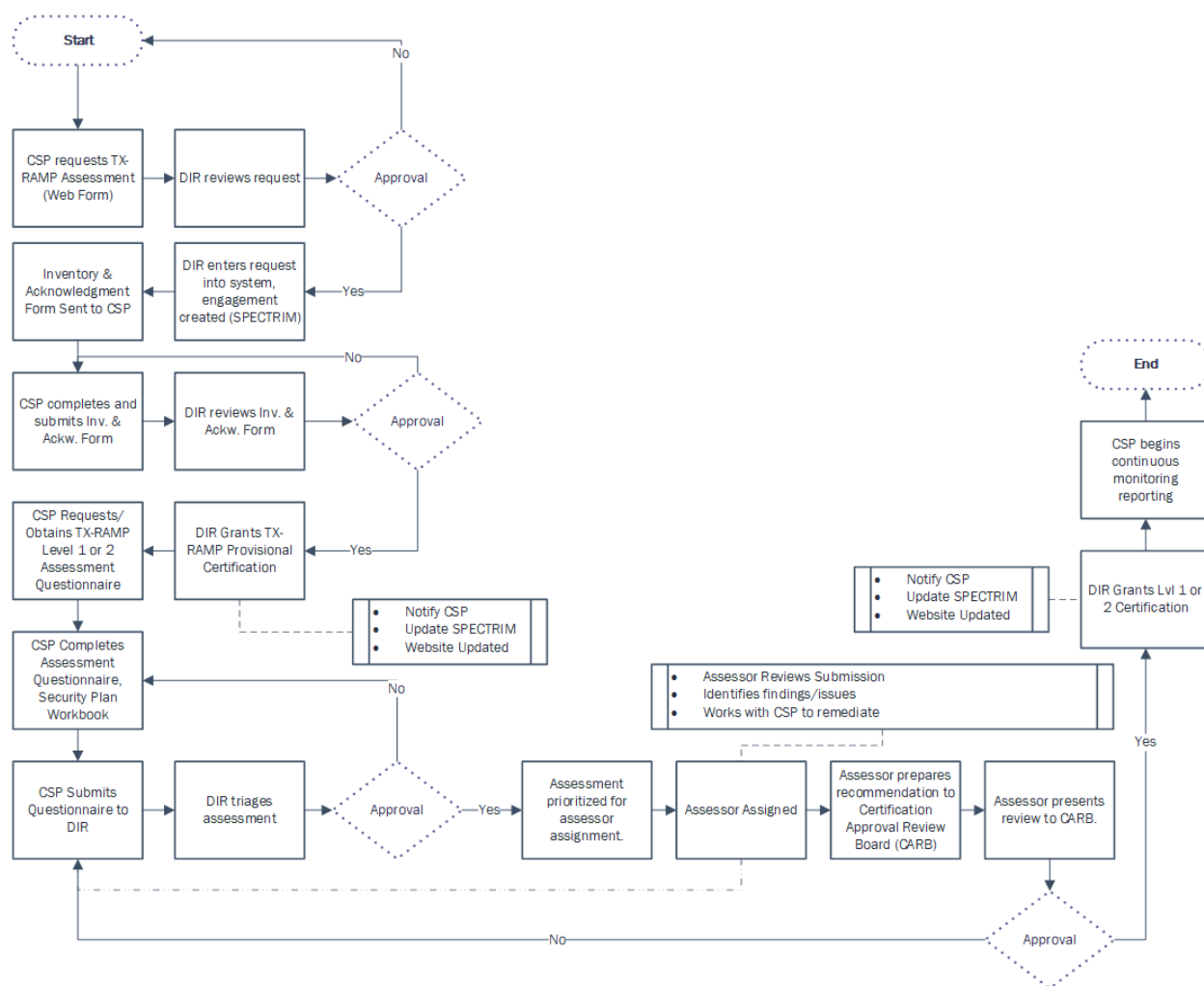
TX-RAMP requires cloud computing service providers to submit information related to their security controls (and their implementation and practices of these controls) to DIR for review and approval through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM).

SPECTRIM provides a mechanism for Policy and Governance staff to track TX-RAMP requests, collect assessment responses, update certification statuses and dates, and generally usher a cloud computing service from intake to certification through ongoing continuous monitoring processes. SPECTRIM enables the direct collection of assessment response and artifacts through a vendor questionnaire functionality, ensuring the separation of state data from external users.

The following flowchart shows the workflow process for a cloud service provider (CSP) to gain TX-RAMP certification.

²⁰⁹ [1 Tex. Admin. Code Chapter 202](#).

Figure 50 Workflow Process for CSP to Gain TX-RAMP Certification



Regional Security Operations Center (RSOC) Processes

In 2022, DIR and Angelo State University signed an interagency contract to bring cybersecurity support to the West Texas economic region by way of the initial RSOC. The Deputy Chief Information Security Officer of the Security Operations/Cybersecurity Incident Response Team (CIRT) and the Statewide Incident Response Coordinator are the primary team members responsible for overseeing the RSOCs, though any of the team may be called upon to support the completion of this objective. For example, the CIRT Team Lead may be required to facilitate a weekly check-in, or the Technical Writer may be called upon to document RSOC processes and procedures.

RSOC Onboarding Process

To establish the pilot RSOC, DIR first solicited interest from public universities through an expression of interest process. After thoroughly reviewing the expressions of interest submitted, DIR selected the university with whom to partner to host the pilot RSOC. RSOCs are planned—but not mandated—to cover each of the state's economic regions as identified by the Texas Comptroller of Public Accounts, depending on legislative approval during upcoming

legislative sessions. To establish additional RSOCs, DIR may use the expression of interest process or determine that another method of selection is appropriate. After a university is selected, DIR and the university collaborate to develop and sign an interagency contract that outlines the services, funding, reporting, and operational expectations of DIR and the university.

After the interagency contract is signed and the RSOC has been established, the Deputy Chief Information Security Officer of Security Operations/CIRT and the Statewide Incident Response Coordinator collaborate with the university during weekly status check-ins to assist in the development and implementation of the center. During these meetings, the Deputy Chief Information Security Officer of Security Operations/CIRT and the Statewide Incident Response Coordinator review key performance indicators, including customer engagement strategy, staffing levels, student worker recruitment and training, curriculum development, the development of an effective monitoring and alerting tooling solution, and physical development of the RSOC. The Deputy Chief Information Security Officer of Security Operations/CIRT and the Statewide Incident Response Coordinator provide direction to the RSOC and identify next steps and goals for the RSOC to work towards.

As the RSOC becomes operational, the Statewide Incident Response Coordinator and CIRT Team Lead provide training and guidance on incident response preparedness, incident handling, and the development of reporting and alert metrics. The CIRT collaboratively prepares this training and guidance, and provides it to the RSOC staff at weekly check-ins.

The Deputy Chief Information Security Officer of Security Operations/CIRT and the Statewide Incident Response Coordinator receive and review the budget and operations reports at both monthly and quarterly intervals to ensure that the university is complying with the interagency contract and consistently providing quality services to RSOC customers.

Volunteer Incident Response Team (VIRT) Processes

If a major cybersecurity incident occurs in Texas, the VIRT provides a method for individuals with the necessary skills and expertise in cybersecurity incident response to support statewide incident management efforts and provide rapid assistance to requesting eligible entities. DIR may deploy the VIRT to assist if: the Governor declares a state of disaster caused by a cybersecurity incident or if a cybersecurity incident occurs that affects multiple participating entities.

DIR's Deputy Chief Information Security Officer of Security Operations/CIRT and a Senior Cybersecurity Analyst recruit VIRT members at outreach events such as the Information Security Forum (ISF) conference and Texas Information Sharing and Analysis Organization (TX-ISAO) meetings, through social media, and via word of mouth. VIRT members cannot be activated until they have completed a background check and signed a non-disclosure agreement. DIR has recruited 104 volunteers, 49 of whom are currently approved for activation.

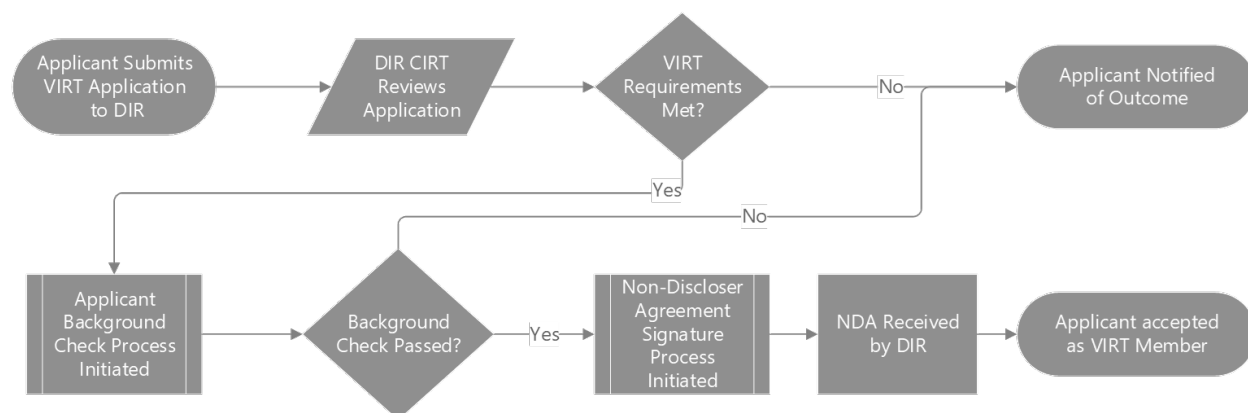
To maintain engagement and build familiarity with the team members, the VIRT holds quarterly meetings wherein members are provided an update of currently available tools and training opportunities as well as a current threat intelligence briefing of Texas' cybersecurity landscape.

The Senior Cybersecurity Analyst is primarily responsible for overseeing VIRT engagement activities and recruitment.

VIRT Application Process

The flowchart below summarizes the VIRT application process.

Figure 51 VIRT Application Process



Cybersecurity Incident Response Team (CIRT) Incident Response Processes

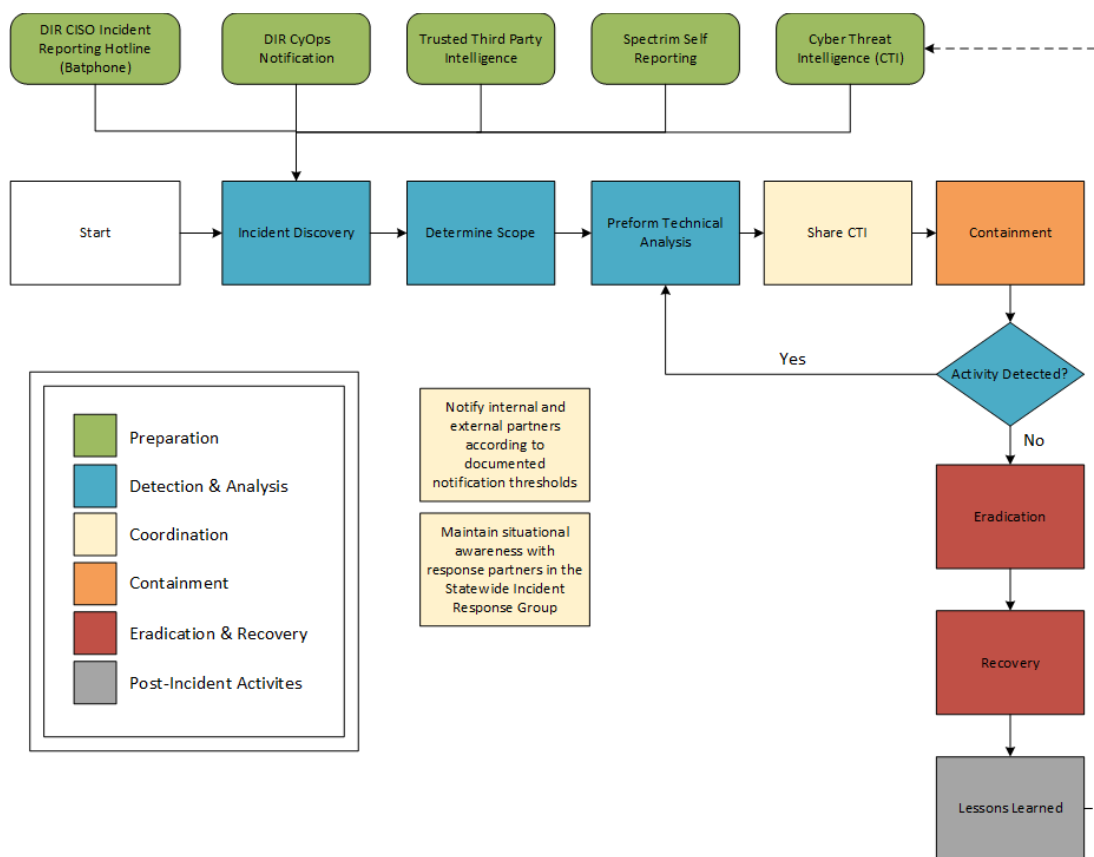
The CIRT's Cybersecurity Analysts are responsible for intaking notifications of cybersecurity incidents. After notification of a cybersecurity incident, the Cybersecurity Analysts contact the impacted entity to confirm the notification, determine the incident's severity level, and provide support remotely by phone or teleconference unless the impacted entity requests onsite support. If the entity requests onsite support, the Deputy Chief Information Security Officer of Security Operations/CIRT will determine whether the CIRT currently has the capacity to fulfill the request. The Deputy Chief Information Security Officer of Security Operations/CIRT may meet with the Chief Information Security Officer as necessary to gauge whether onsite resources may be provided.

While working to contain a cybersecurity incident, the Cybersecurity Analysts provide technical assistance to the impacted entity, including information and advice regarding system configuration, cybersecurity best practices, threat actor mitigation, and next steps for getting the impacted entity's systems back online.

Once the incident is fully contained and the impacted entity has begun post-incident activities, the Cybersecurity Analysts analyze previously gathered digital images of the compromised systems for threat intelligence that can be distributed to members of the TX-ISAO or wider cybersecurity community to prevent another cyberattack.

The chart below illustrates the incident response process.

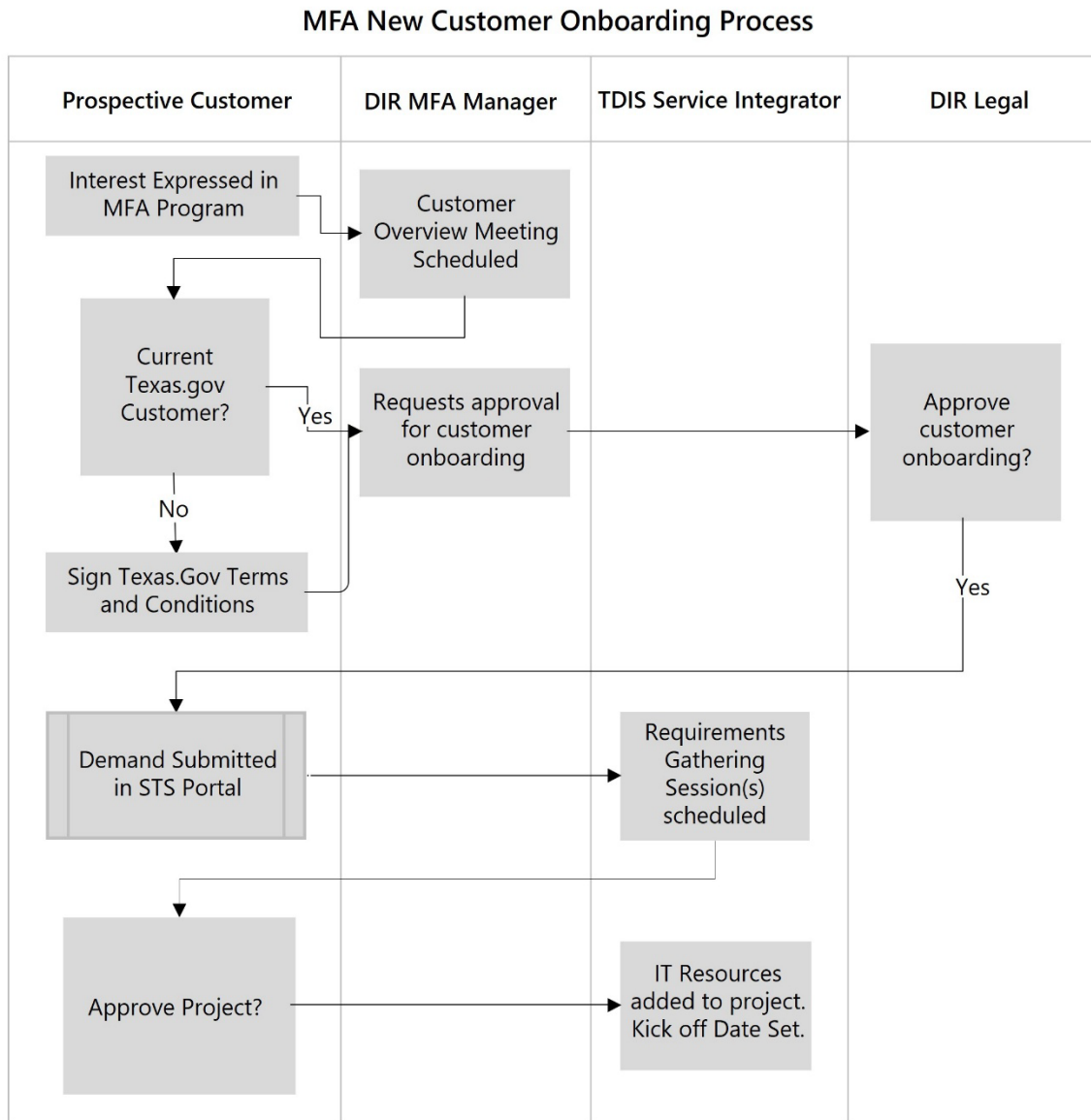
Figure 52 CIRT Incident Response Process



Multi-factor Authentication (MFA) Onboarding Process

The flowchart below describes the onboarding process for new customers into the DIR MFA program.

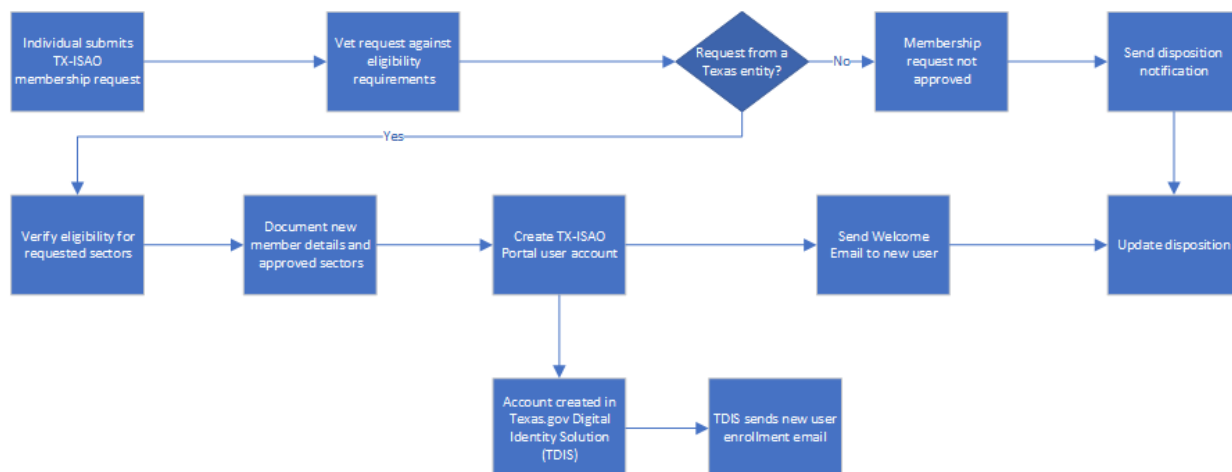
Figure 53 New Customer Onboarding Process



Cybersecurity Coordination Processes

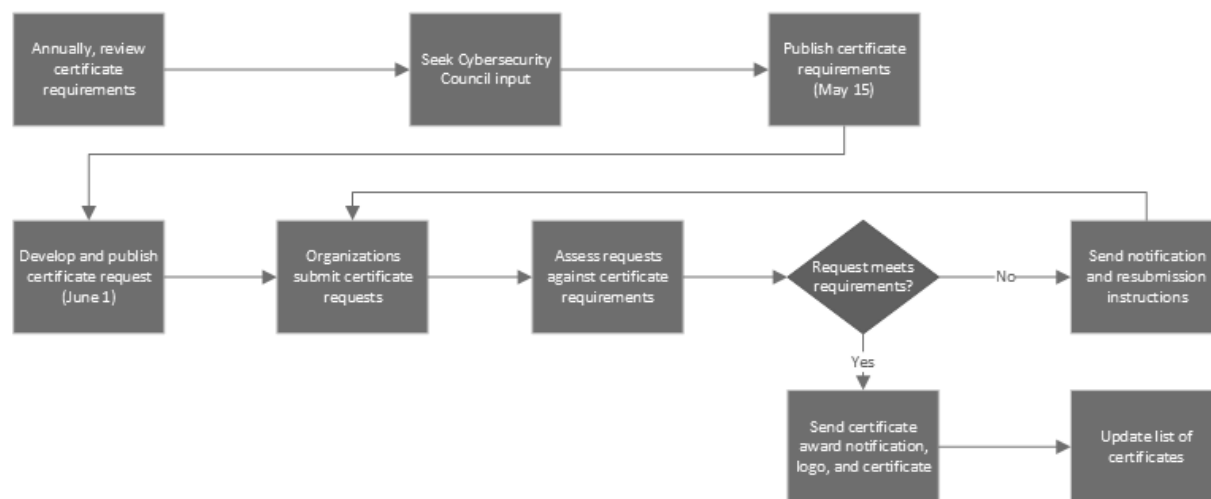
The following flowchart shows the workflow process for onboarding a new Texas Information Sharing and Analysis Organization member.

Figure 54 Onboarding Process for New TX-ISAO Member



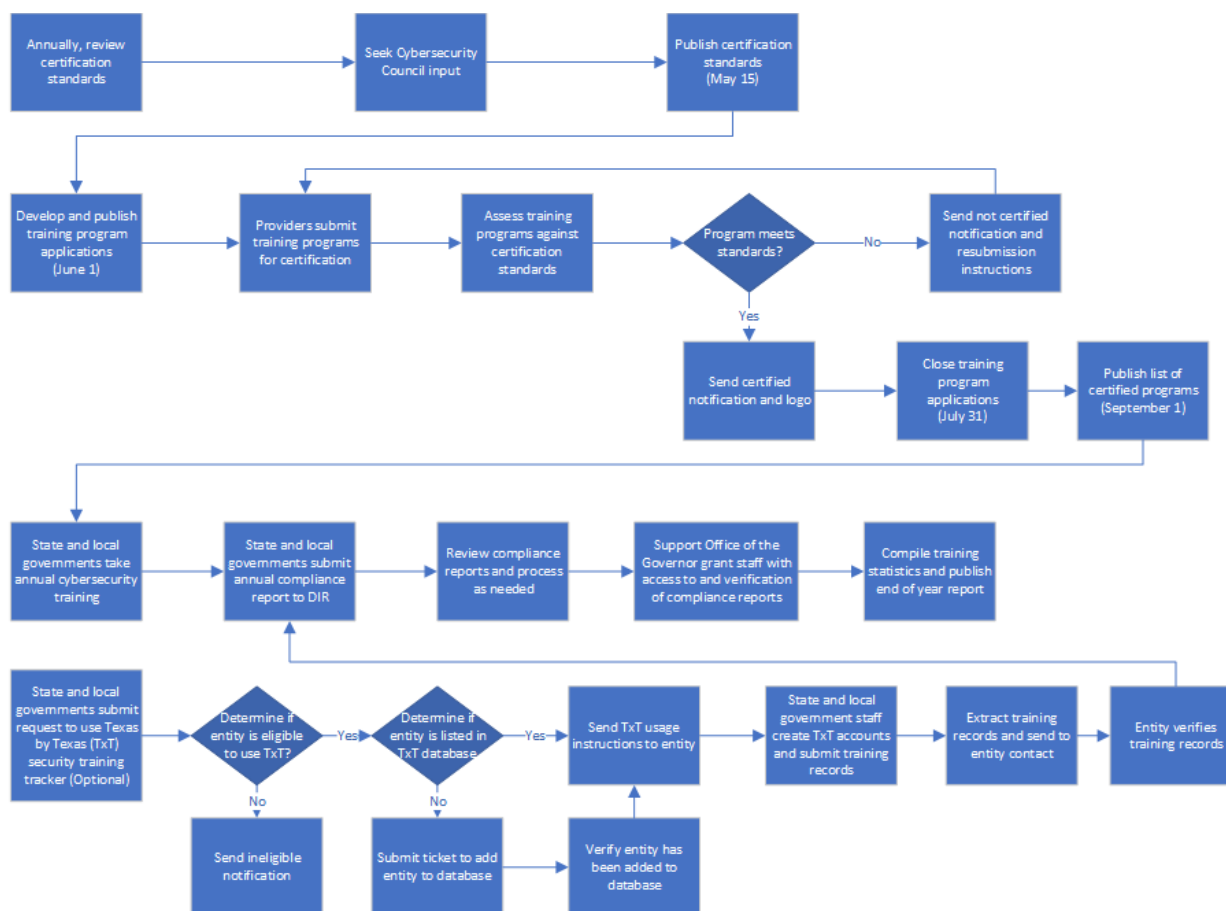
The following flowchart shows the workflow process for an organization to be awarded a Texas Cyberstar Certificate.

Figure 55 Workflow Process to Be Awarded a Texas Cyberstar Certificate



The following shows the workflow process for an organization to take and report annual security awareness training.

Figure 56 Workflow Process for Annual Security Awareness Training



g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The majority of cybersecurity funds are allocated to: Regional Security Operations Centers (RSOCs); multi-factor authentication (MFA) for state agencies and institutions of higher education; endpoint detection and response (EDR) software for state agencies; cybersecurity assessments; and penetration tests for state agencies and institutions of higher education. The original appropriation in the GAA for most cybersecurity services was General Revenue but in accordance with Rider 11 in DIR's bill pattern, and in an effort to be responsible stewards of taxpayer money, the agency returned General Revenue and funded these services through the collected revenues in the chart below.

Strategy	Method of Finance	Amount
C.1.1 - Security Policy and Awareness	Clearing Fund	\$921,150
C.1.2 - Security Services	Clearing Fund	\$12,989,401
C.1.2 - Security Services	Telecommunications Revolving Account	\$9,977,973
C.1.2 - Security Services	Federal Funds	\$408,120
C.1.2 - Security Services	General Revenue	\$541,004

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

Cyber threat actors are continuously improving their brute strength, sophistication, and hacking resources. Protecting the state (and the nation) from cyber threats requires coordination between entities at every level of government. Collaboration in the cybersecurity field is paramount, which is the reason so many entities exist that offer similar services. While cybersecurity is—and will always remain—a shared responsibility, no other state agency or program provides the volume and variety of cybersecurity services that DIR delivers to Texas' public sector, nor does any other agency possess the complex knowledge of the technology field and Texas' network security system that is required to be an effective leader of Texas' cybersecurity strategy and incident response. DIR is Texas' designated agency for cybersecurity with more statutory jurisdiction regarding cybersecurity matters than any other state agency.

For convenience, this section has been divided by function objective.

Cybersecurity Protection, Prevention, and Response

As previously identified, DIR provides cybersecurity resources to the state of Texas through several teams and programs. Each team or program offers varying cybersecurity services with minimal overlap. While other state agencies monitor their own systems and infrastructure for cyber threats and other cybersecurity issues, DIR provides and coordinates a centralized repository of cybersecurity resources and expertise that other state agencies can access to augment their own internal cybersecurity operations.

DIR Internal Overlap

DIR's Cybersecurity function is shared by OCISO and the Cybersecurity Operations team, but while OCISO and the Cybersecurity Operations team collaborate, their duties differ.

The Cybersecurity Operations team responds to security incidents at state agencies protected by the NSOC whereas OCISO oversees incident response for state agencies not on the state's network, local governments, school districts, and other local entities.

While both can provide boots on the ground support in the event of an incident, both teams have clearly delineated roles and responsibilities in response assistance to not have any gaps or overlaps.

OCISO has a broader, more governance-based foundation, working to improve security for the state as a whole. OCISO provides services to assist government entities strengthen their cybersecurity posture through policy guidance and educational opportunities. The Cybersecurity Operations team focuses on protecting state agencies on the state's network.

The Cybersecurity Incident Response Team (CIRT) and DIR's Managed Security Services (MSS) offer similar services. Most entities impacted by ransomware and other cybersecurity incidents across Texas usually do not have sufficient budgets for cybersecurity, which is a major factor in their being targeted by threat actors in the first place. The CIRT provides similar offerings as the provider but at zero cost. MSS offerings are priced at a highly competitive rate; however, smaller local government entities may not be able to afford these first-class services with their minimal budgets. The CIRT's free services overcome the smaller local government entities' budget limitations when an unexpected cybersecurity incident occurs.

Without the CIRT and the CIRT's programs such as the RSOCs, these impacted entities would have few, if any, options available for cybersecurity incident response assistance from government. The CIRT serves as a single, centralized source of guidance and technical expertise for those entities.

The CIRT often connects entities to the MSS contract based on need and budget.

State and Local Government Entity Overlap

The Texas Department of Public Safety and the Texas Military Department also provide support to state agencies and local governments in response to cybersecurity attacks, but these agencies' support is more narrowly focused than DIR's cybersecurity incident response. The Texas Department of Public Safety's cybersecurity incident response capabilities address cybersecurity incidents impacting law enforcement entities while the Texas Military Department only deploys support when authorized by the Governor.

The Public Utilities Commission and the Electric Reliability Council of Texas (ERCOT) operate the Texas Cybersecurity Monitor Program.²¹⁰ The cybersecurity monitor is tasked with managing a cybersecurity outreach program, communicating emerging threats and best business practices, reviewing cybersecurity self-assessments, researching, and developing best business practices for cybersecurity, and reporting to the Public Utilities Commission on cybersecurity preparedness for monitored utilities. In addition to monitored utilities, an electric utility, municipally owned utility, or electric cooperative operating solely outside the ERCOT region (non-ERCOT utility) may elect to participate in the [Texas Cybersecurity Monitor Program](#).

Some institutions of higher education provide support for community cybersecurity programs (such as the University of Texas at San Antonio and Texas A&M University). However, these programs tend to target a particular region or sector, whereas the DIR services are available

²¹⁰ [Tex. Util. Code § 39.1516](#).

statewide.

DIR partners with the Texas Education Agency and, by extension, the 20 Education Service Centers in Texas to provide cybersecurity support to the K-12 schools of Texas.

Some local government stakeholder organizations provide basic cybersecurity support and education to their members (such as the Texas Municipal League, Texas Association of Counties, Texas Education Agency, and Texas Association of Regional Councils). However, the services offered by these organizations are less comprehensive than DIR's offerings.

Federal Government Entity Overlap

DIR partners with the federal Cybersecurity and Infrastructure Security Agency (CISA)—an operational component of the Department of Homeland Security—to minimize duplication of efforts and to present a unified message to the local governments of Texas. DIR shares CISA's threat alerts and bulletins to all Texas Information Sharing and Analysis Organization (TX-ISAO) members and collaborates with CISA on joint educational presentation opportunities.

CISA's primary scope is on a federal level, including the exploration of cybersecurity attacks as they occur across different states. CISA is focused on the big picture of cybersecurity at the federal level and does not provide hands-on incident response. CISA provides threat information, and certain assessment and penetration testing services to government entities across the country. The approximate wait time for a cybersecurity assessment from CISA is one year.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) shares generalized threat intelligence that is not specific to Texas. MS-ISAC offers limited paid cybersecurity monitoring and does not provide onsite assistance. The MS-ISAC has a much larger scope than DIR (multiple states as its name suggests), and thus, does not get involved with "minor" cybersecurity incidents suffered by entities in the state of Texas.

MS-ISAC and CISA do not always have the capability to go onsite to respond to incidents, given their expansive federal jurisdiction. DIR, however, can deploy onsite staff in response to cybersecurity incidents since DIR's jurisdiction is limited to Texas.

Other External Overlap

Cyber risk pools and cyber insurance focus on the liability associated with potential cybersecurity incidents. These liability protections may not support entity mitigation or recovery efforts. Additionally, cyber risk pools and cyber insurance have a history of paying ransomware demands, which only incentivizes further threat actor activity.

Cybersecurity Policies and Guidance

DIR provides guidance to government entities related to cybersecurity best practices. Several organizations provide such guidance within the private sector, public sector working groups, and the federal government. However, DIR focuses on Texas-specific information security requirements whereas other advisory-type organizations typically provide guidance specific to

the requirements of the regulation or best practice of a particular focus area.

There are many third-party information security validation programs that serve a similar function to the Texas Risk and Authorization Management Program (TX-RAMP). These programs include:

- **Federal Risk and Authorization Management Program (FedRAMP):** FedRAMP has been in existence since 2011 with the goal of centralizing the authorization process for federal agencies that are leveraging cloud services. This program is federal specific but served as a model for the state-level implementation of TX-RAMP.
- **State Risk and Authorization Management Program (StateRAMP):** StateRAMP is a non-government organization that emerged contemporarily with TX-RAMP. The goal of StateRAMP is to provide similar centralized authorization services to state and local governments as FedRAMP focuses only on cloud services used by federal agencies.
- **Cloud Security Alliance (CSA):** CSA focuses on promoting best practices for cloud security along with assessment criteria and a validation program to indicate the security practices of cloud service providers. The CSA Security, Trust, and Assurance Registry (STAR) provides a framework for cloud service providers to document and disclose their security controls and practices. It includes a self-assessment questionnaire and a third-party certification option called STAR Certification.
- **American Institute of Certified Public Accountants (AICPA) Service Organization Control II** The AICPA sets the standards used to assess and provide assurance over the security, availability, processing integrity, confidentiality, and privacy of data within service organizations.

Cybersecurity Training and Outreach

CISA provides educational opportunities to government entities across the country.

- i) **Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.**

DIR works with stakeholder organizations to receive input on the needs of their members, coordinate efforts, and support and expand upon member initiatives as applicable. Coordination is achieved by attending stakeholder meetings and inviting representatives to participate in DIR efforts. Examples include, but are not limited to:

- Attending monthly preparedness calls with the Texas Association of Regional Councils and councils of government.
- Attending quarterly Texas Critical Infrastructure Protection (TCIP) Task Force meetings.

- Attending Texas Municipal League and Texas Association of Counties annual conferences.
- Attending the Texas Education Agency Cybersecurity Coordinator Forum.
- Including local governments in OCISO strategic planning sessions.
- Including stakeholder representatives on the Texas Cybersecurity Council.

DIR has a member on the Multi-State Information Sharing and Analysis Center (MS-ISAC) education and awareness committee to help provide input and direction on outputs from this organization. In addition, DIR's Chief Information Security Officer serves on the MS-ISAC executive committee to help provide input into the overall services which MS-ISAC delivers.

DIR partners with four institutions of higher education via memorandums of understanding or interagency agreements to operationalize the Texas Information Sharing and Analysis Organization (TX-ISAO) and deliver initiatives. This collaboration supports ongoing communications and program alignment. These universities include:

- University of Texas at San Antonio (TX-ISAO Partner and DIR initiatives): Cybersecurity training for election officials;
- Texas A&M University (TX-ISAO Partner);
- University of Texas at Austin (TX-ISAO Partner); and
- Texas A&M Engineering Extension Service (DIR initiatives): Tabletop exercise development; Introduction to Cyber Incident Investigation for Law Enforcement course.

TX-RAMP currently accepts FedRAMP and StateRAMP authorizations in lieu of undergoing the TX-RAMP assessment and certification process. These programs are built on underlying common criteria, and all have similar goals and objectives. Depending on the customer base of a cloud computing service provider, it may be more practical to seek TX-RAMP certification if that provider is only servicing Texas state agencies and institutions of higher education. 1 Texas Administrative Code Sections [202.27](#) and [202.77](#) and the TX-RAMP Program Manual specify the mandatory standards and control baselines required for cloud computing services to receive TX-RAMP certification and maintain compliance with the program.²¹¹

Additional third-party assessment and audit assurances may be taken into consideration when determining TX-RAMP certification but, as of July 2023, DIR has not accepted any other program assurances in lieu of completing certain TX-RAMP assessments and certification processes.

²¹¹ 1 Tex. Admin. Code §§ [202.27](#), [202.77](#).

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

Eligible local, regional, or federal units of government of the Cybersecurity function include:

- Local governments, including counties, municipalities, school districts, and junior college districts;²¹²
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.²¹³

DIR's Cybersecurity function requires the establishment of working relationships with local, regional, and federal government entities.

Cybersecurity Incident Response

As previously identified, DIR provides incident response support to local governments, K-12 school districts, public junior colleges, institutions of higher education, special districts, and state agencies.

DIR actively participates in cybersecurity information sharing with:

- Cybersecurity and Infrastructure Security Agency (CISA);
- Department of Homeland Security (DHS);
- Federal Bureau of Intelligence (FBI);
- U.S. Computer Emergency Readiness Team (US-CERT);
- Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Center for Internet Security (CIS);
- U.S. Secret Service;
- Texas Military Department;
- DIR's vendor partners;
- Network Security Operations Center (NSOC) security tools;
- Security industry researchers;
- State agencies; and
- Texas institutions of higher education.

²¹² [Gov't Code § 2054.003\(9\)](#).

²¹³ [Gov't Code § 2157.068\(j\)](#); *see also* [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\)](#).

Texas Information Sharing and Analysis Organization (TX-ISAO)

The TX-ISAO is open to any Texas entity including state agencies, local governments, public and private institutions of higher education, and the private sector. Many of these entities are TX-ISAO members and benefit from intelligence and services.

Cybersecurity Education and Information Security Forum (ISF)

DIR provides educational opportunities via webinars and the ISF conference to all Texas public sector organizations. A member of the Security Services team serves on the education and awareness committee for the Multi-State Information Sharing and Analysis Center (MS-ISAC), a CISA organization.

State and Local Cybersecurity Grant Program (SLCGP)

The State and Local Cybersecurity Grant Program (SLCGP), through the Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA), appropriated \$1 billion over four years (2022-2025) to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments. Texas was allocated approximately \$40 million over those four years.

The Office of the Governor (OOG) is the State Administrative Agency and serves as the fiscal agent and authorizing official of the SLCGP federal funds. OOG submitted the FY22 SLCGP application to DHS and will submit subsequent applications.

DIR serves as the subject matter expert in Texas pertaining to all programmatic requirements and federal regulations associated with the SLCGP. DIR provided assistance to OOG in the development of the annual federal SLCGP application.

Local governments are eligible sub-recipients. Per [6 U.S.C. Section 101\(13\)](#), local governments are defined as:

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government.
- A rural community, unincorporated town or village, or other public entity.

DIR established a Cybersecurity Planning Committee, comprised of representatives from cities, towns, and counties; rural, suburban, and urban areas; higher education and K-12 public education; and public health and safety sectors. DIR's State Cybersecurity Coordinator serves as committee chair. The planning committee is responsible for developing, implementing, and revising the state's Cybersecurity Plans and formally approving the Cybersecurity Plan (along with the state Chief Information Officer and state Chief Information Security Officer).

OOG will submit the state Cybersecurity Plan to DHS. DIR will work with OOG to develop the application process for local governments to submit projects. Upon DHS's approval of the

Cybersecurity Plan, OOG will publish a request for applications. The Cybersecurity Planning Committee will review the project submissions and assist with the determination of effective funding priorities (i.e., work with entities within the eligible entity's jurisdiction to identify and prioritize individual projects).

OOG will administer sub-recipient grants, including issuing subawards, disbursing funds to subrecipients, tracking subrecipient financial and programmatic performance, and conducting financial and programmatic monitoring of subrecipients.

k) If contracted expenditures are made through this program please provide:

A Short Summary of The General Purpose of Those Contracts Overall

The contracts in this program are primarily used for delivering cybersecurity services, such as assessments, penetration tests, multi-factor authentication (MFA), end-point detection and response (EDR) services, and regional security operations centers.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$22.2 million in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 40 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from September 2020 through August 2022 for these contracts. The funding sources for these contracts include revenues from the Cooperative Contracts and communications and technology services programs in addition to general revenue and federal funds.

The Method Used to Procure Those Contracts

The methods used to procure these contracts include interagency contracts, invitation for bids, request for quote, request for qualifications, request for offers, and Cooperative Contracts.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-MSS-SCP-001	AT&T	Managed Security Services Service Component Providers contract for shared technology services program.	\$11,138,790.38
RSOC Interagency Contract	Angelo State University	Interagency Contract for Regional Security Operations Center.	\$3,000,000.00
DIR-TSO-4318/SOW-01-FY-21-0004	GTS Technology Solutions Inc.	Provides software-as-a-service and RSA technical support for Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) program within OCISO program.	\$1,713,358.72
DIR-ESS-TGOV-SVCS-254	Deloitte Consulting LLP	Provides Texas.gov Services for shared technology services program.	\$1,446,577.61
DIR-TSO-4006/DIR-ECM-IAT-SOW-4006	Learning Tree International USA Inc	Provides DIR InfoSec Academy Education and training services for OCISO program	\$856,675.00

The Methods Used to Ensure Accountability for Funding and Performance

Contracts are assigned Contract Managers who work with program staff to ensure that vendors are delivering services and performing in accordance with the contracts.

A Short Description of Any Current Contracting Problems.

Not applicable.

l) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

DIR identifies the following six barriers and challenges impeding the Cybersecurity function.

Barrier 1: Statutory Ambiguity

As discussed in IX. Major Issues, DIR draws its statutory authority to operate the Managed

Security Services (MSS) program from Government Code Section 2059.104,²¹⁴ Government Code Chapter 2054,²¹⁵ and discrete sections of the biennial appropriations acts. Specifying and consolidating DIR's authority for the MSS program would provide increased clarity.

Government Code Section 2054.52005²¹⁶ authorizes DIR to deploy the Volunteer Incident Response Team (VIRT) to provide assistance under DIR's direction and "the managed security services framework established under [Government Code Section 2054.0594\(d\)](#) [may] assist when a cybersecurity event affects multiple entities or the Governor declares a state of a disaster caused in response to a cybersecurity event."²¹⁷

However, [Government Code Section 2054.0594\(d\)](#) does not establish a managed security services framework. This section directs DIR to establish "a framework for regional cybersecurity working groups to execute mutual aid agreements that allow state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the incident response team established under Subchapter N-2 to assist with responding to a cybersecurity event in this state."²¹⁸ Thus, the reference appears to suffer from a drafting error that creates significant ambiguity regarding DIR's authority.

As discussed in IX. Major Issues, Government Code Section 2054.515(a)(2) requires agencies to conduct an information security assessment that includes an assessment of the agency's data governance program with assistance from the agency's Data Management Officer.²¹⁹ Information security and data governance are separate concepts that require unique analysis. Separating the data governance assessment from the security assessment in statute would provide clarity and a separation of the two different functions in alignment with best practices of these discrete fields.

Additionally, Government Code [Section 2054.515](#), which requires agencies to submit their agency security assessment results to DIR, contains two subsections with differing report submission deadlines: November 15 of each even-numbered year, December 1 of each even-numbered year, or 60 days after the date of the assessment's completion.²²⁰

Barrier 2: Unclear Mandatory Cybersecurity Training Requirements

Government Code [Section 2054.5191](#) requires mandatory cybersecurity training for all state and local government employees that use a computer to complete or perform at least 25

²¹⁴ [Gov't Code § 2059.104](#).

²¹⁵ [Gov't Code Chapter 2054](#).

²¹⁶ [Gov't Code § 2054.52005](#).

²¹⁷ [Gov't Code § 2054.0594\(d\)](#).

²¹⁸ [Gov't Code § 2054.0594\(d\)](#).

²¹⁹ [Gov't Code § 2054.515\(a\)\(2\)](#).

²²⁰ [Gov't Code § 2054.515](#).

percent of their duties.²²¹ This threshold is difficult to measure and gives discretion to local governments to determine which employees use computers with sufficient frequency to require them to comply with the statute training mandate. Some local entities have reported that none of their employees use a computer at least 25 percent of the time and, therefore, they do not have to comply with the mandatory training. Additionally, employees with less familiarity with computers are more vulnerable to phishing attacks and other socially engineered cyber threats. Furthermore, Texas Education Code Section 11.175(g) only requires the entity's Cybersecurity Coordinator to complete the cybersecurity training, while allowing the school district to determine which other employees must take the mandatory training.²²² School districts are a growing target of cyber attackers, and the use of technology in educational settings is increasing. As such, all local government—including independent school district—employees that are granted access to the local government's computer system should be required to take the mandatory cybersecurity training.

Barrier 3: Increasing—and Increasingly Sophisticated—Cyber Threats

Cyber threat actors are constantly and continually attacking Texas entities. Because Texas has so much digital infrastructure, it remains an appealing target for cyber threat actors. The cyber threat landscape in Texas, therefore, is tumultuous and oppressive with thousands of attempted cyberattacks occurring daily. Cyber threats continue to increase on an upward trend in addition to becoming more sophisticated and requiring more in-depth analysis to fully comprehend.

DIR's cybersecurity responsibilities have expanded as its programs have matured, adding new technologies, tools, processes, and staff to support this critical function. Traffic in and out of the state networks has also increased. DIR observed an immediate increase in traffic due to the pandemic, which forced many state employees to begin teleworking. In addition, agencies have shifted to using more cloud-based software-as-a-service solutions than ever before. This increased traffic requires more Cybersecurity Analyst hours to investigate and alert agencies of suspicious network activity.

DIR's cybersecurity teams' workloads have proportionately increased as threats, standards, and responsibilities increase. With the continually increasing complexity of regulations, industry standards, and volume of security assessments, the workload can become overwhelming with limited resources and staffing constraints hindering the teams' ability to develop, update, and communicate information security requirements in a timely manner. If current trends continue and without increased staffing, these teams may struggle to keep up with emerging cybersecurity threats, evolving compliance requirements, and the need for ongoing programmatic reviews.

²²¹ [Gov't Code § 2054.5191.](#)

²²² [Educ. Code § 11175\(g\).](#)

Barrier 4: Lack of Statutory Responsibility for Critical Infrastructure

Critical infrastructure is at increased risk of being targeted by cyber threat actors who seek to cause disruption and damage. In Texas, most critical infrastructure entities are owned by private sector entities. Many of the critical service providers that Texas relies on daily do not have to follow cybersecurity requirements, and it is not clear where statutory responsibility lies for the cybersecurity protection of critical infrastructure.

Barrier 5: Complications with Cyber Insurance

Cyber insurance providers work with their policy holders to help limit their liability when they are impacted by a cybersecurity incident. Cyber insurance providers often require impacted organizations to use an approved vendor for incident response support and legal representation. These resources may limit the impacted entity's ability to speak to—or share intel with—DIR, even though sharing indicators of compromise (IOCs) and other attack details could help other entities prevent future attacks.

Barrier 6: Local Government Challenges

Local governments are common targets of cyber attackers due to the likelihood that the entity will not have the cybersecurity resources necessary to combat a cyber threat. The lack of staffing and resources for cybersecurity at the local government level, combined with cyber threat actors' extremely aggressive nature, is a serious issue. Local governments cannot combat cyber threat actors who may have political motivations, are part of organized crime, or are sponsored by—or affiliated with—a foreign state. Regional Security Operations Centers (RSOCs) can provide some assistance, but they cannot solve the problem alone. Additionally, local governments are not required to maintain minimum security standards, have a cybersecurity incident response plan, or maintain points of contact for cybersecurity.

Though DIR can provide cybersecurity assistance to local governments, DIR faces several challenges to improving their cybersecurity posture. In a state as large as Texas, DIR sometimes lacks the personnel needed to communicate DIR's service offerings to all who may need them. Although DIR engages in significant outreach efforts to publicize the tools and services available through DIR, many local entities are still not even aware of DIR, or the free services that DIR provides.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

Awards and Recognitions

In May 2023, DIR received a StateScoop State IT Innovation of the Year Award for the pilot Regional Security Operations Center (RSOC). In 2022, DIR partnered with Angelo State University to operate the pilot RSOC to provide Texas local government entities with cybersecurity support. In addition, in June 2023, DIR received a Best of Texas Award from Government Technology for best IT collaboration project for the pilot RSOC.

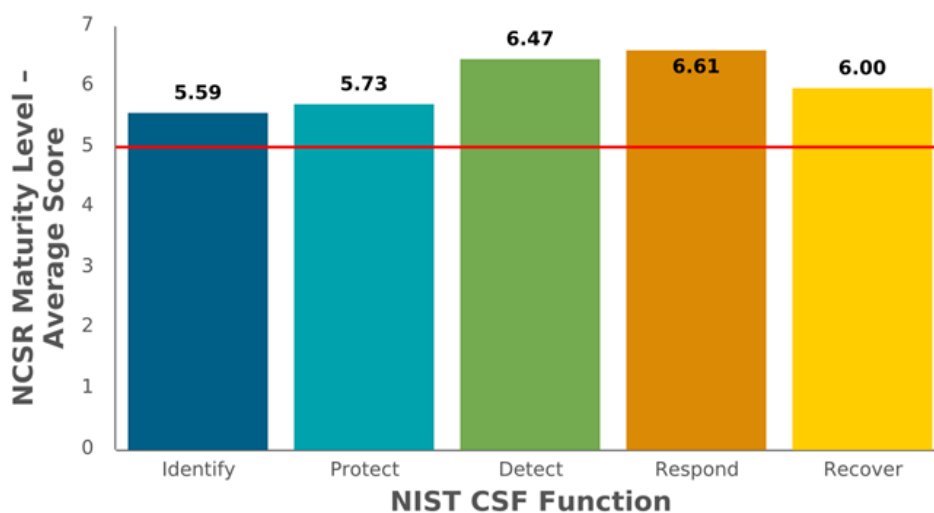
Texas' Chief Information Security Officer Nancy Rainosek received the 2021 Thomas M. Jarrett

State Cybersecurity Leadership Award, which honors state CISOs for exceptional accomplishments in their field.

DIR's Statewide Incident Response Coordinator Jonathan King received the 2021 Rising Star Award from the Texas Association of State Systems for Computing and Communications (TASSCC). The TASSCC Rising Star Award recognizes emerging government technology leaders who have less than 10 years of IT experience and are not in a director or senior-level position. The award is given to individuals who have a track record that reflects a strong potential for continued advancement in the technology arena.

DIR conducts the annual Nationwide Cybersecurity Review (NCSR), a self-assessment of the state's level of cybersecurity maturity as assessed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework functions. The below chart indicates DIR's score.

Figure 57 DIR's 2022 NCSR Self-Assessment Results



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

Managed Security Services (MSS) is an offering within DIR's Shared Technology Services program to provide strong and consistent management of state data security. This video provides an overview of MSS: <https://youtu.be/OftnF4LZt70>.

o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility). For each regulatory program, if applicable, describe:

DIR monitors compliance with the following requirements related to the Cybersecurity function.

Designating an Information Security Officer

Why the Regulation Is Needed

Information Security Officers (ISOs) have specific responsibilities identified in TAC 202.²²³ As DIR's primary point of contact for a state agency's information security matters, accurate ISO designation and contact information ensures that DIR can directly and unerringly make contact should a cyber threat or cybersecurity incident arise. In addition, ISOs are charged with certain reporting requirements, including the biennial security plan and the annual end user training completion. DIR conducts outreach to ISOs before and after those required reports are due to ensure agencies complete those deliverables.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

Agencies complete [a short form on the DIR website](#) to designate an ISO. When this form is submitted, DIR gets notified and updates the internal system of record. In addition, DIR sends out a welcome email that contains information necessary for a new ISO. DIR will also have the new ISO added to the security-officer mailing list and into SPECTRIM.

Follow-up Activities Conducted When Non-compliance Is Identified

DIR conducts a regular review (at least annually) to ensure the record of truth is accurate. If a designation is not accurate, DIR reaches out to the agency to update the record.

Actions Available to the Agency to Ensure Compliance

DIR does not have authority to create a finding or penalty.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Security Assessments

Why the Regulation Is Needed

State agencies are required to conduct biennial security assessments.²²⁴ Assessments are a crucial tool in helping agencies understand where their security program is excelling and failing. Security assessments also help agencies build a strategic roadmap to reduce gaps and potentially justify requests for additional resources for potential cybersecurity projects. DIR provides security assessments based on the Texas Cybersecurity Framework (TCF) to help agencies meet this requirement.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

The assessment must include information resources systems, network systems, digital data

²²³ [1 Tex. Admin. Code Chapter 212.](#)

²²⁴ [Gov't Code § 2054.515.](#)

storage systems, digital data security measures, and information resources vulnerabilities. The TCF assessment covers these areas through the 42 control objectives identified in the TCF.

Follow-up Activities Conducted When Non-compliance Is Identified

Agencies are required to send their assessment report to DIR. For assessments funded by DIR, DIR receives a copy from the Managed Security Services service provider upon completion. For those agencies that get assessments outside of the DIR-funded option, DIR works with them to send a secure copy to DIR for compliance.

Actions Available to the Agency to Ensure Compliance

DIR does not have authority to create a finding or penalty; however, this would be considered an audit finding for the agency should assessments be in scope for the audit.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Data Management



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by **leading the state's technology strategy**, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.

a) Provide the following information at the beginning of each program description.

Name of Program or Function: Office of the Chief Data Officer

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Neil Cooke, Statewide Chief Data Officer

Statutory Citation for Program:

[Government Code Chapter 2054, Subchapter B, Administration of Department](#)

[Government Code Chapter 2054, Subchapter C, General Powers and Duties of Department](#)

[Government Code Chapter 2054, Subchapter F, Other Powers and Duties of Department](#)

[Government Code Chapter 2060, Interagency Data Transparency Commission](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.

Operational
Excellence



The objective of DIR's Data Management function is to promote a data sharing culture throughout state government and higher education by:

- Strengthening data governance by implementing best practices, appointing dedicated data management staff, and maturing data management programs.
- Enhancing data security and privacy through strong controls based on risk and legal requirements.
- Facilitating better decisions by adopting flexible analytics that provide leaders with business-oriented data.
- Fostering a data-sharing culture where open data is readily available, enabling state leaders and the public to make data-driven decisions.

The Office of the Chief Data Officer (OCDO) coordinates the Texas Statewide Data Program, which provides leadership and fosters collaboration between state agencies, local governments, other states, and institutions of higher education to establish statewide data management strategic direction and best practices for DIR's customers. The statutorily designated Chief Data Officer²²⁵ directs the key Data Management function.

The major activities performed under the Data Management function include:

- **Managing the Texas Statewide Data Program.** The OCDO coordinates the Texas Statewide Data Program to promote a data sharing culture throughout state government and higher education. The Texas Statewide Data Program improves data governance and integrity statewide, provides opportunities for data sharing across government, and works with state agencies and institutions of higher education to collaboratively develop data policies, standards, and best practices.
- **Administering the Texas Open Data Portal.** The OCDO provides leadership and guidance to state agencies on the use of the Open Data Portal to publish data. The Open Data Portal team is responsible for the day-to-day operations and management of the Open Data Portal, including granting access and publishing rights to customers, managing the dataset inventory, providing guidance on open data governance, serving as a liaison between customers and the open data vendor-partner, and facilitating individual open data review/design sessions and the quarterly Open Data Portal User Group meetings to highlight best practices of open data selection, preparation, and publishing.

²²⁵ [Gov't Code § 2054.0286.](#)

- **Administering the Texas Closed Data Portal.** The OCDO assists DIR customers in exploring the broader adoption of the Closed Data Portal, which allows state agencies to share sensitive or confidential information in a secure environment with restricted access. The OCDO is responsible for assisting agencies in the setup and design of Closed Data Portal instances, including best practices for sharing private data.
- **Establishing interagency data sharing standards.** In 2018, the Texas Statewide Data Program established the Texas Statewide Data Exchange Compact to facilitate a consistent method of compliance with state and federal laws and regulations regarding data sharing and data security. The Texas Statewide Data Exchange Compact is a uniform data sharing and data security agreement for participating Texas state agencies and institutions of higher education. This agreement contains the standard terms and conditions applicable to all agencies interested in data sharing and exchange. Once executed by all parties, the Texas Statewide Data Exchange Compact enables a more efficient and effective process for sharing data.
- **Leading and facilitating the Data Management Advisory Committee.** In 2021, the Legislature passed [Senate Bill 475](#), which tasked the DIR Board with appointing a Data Management Advisory Committee composed of each Data Management Officer designated by a state agency. The advisory committee's responsibilities include advising the DIR Board and DIR on establishing statewide data ethics, principles, goals, strategies, standards, and architecture; providing guidance and recommendations on governing and managing state agency data and data management systems, including recommendations to assist Data Management Officers in fulfilling their statutory duties; and establishing performance objectives for state agencies. The Chief Data Officer facilitates a quarterly meeting with advisory committee members to ensure effective communication, collaboration, and decision-making while aligning with the state's data management goals and objectives and maintaining compliance with regulations and standards.
- **Establishing and managing the Texas Data Literacy Program.** The OCDO manages the Texas Data Literacy Program to provide guidance, training, and education on topics related to data management, open data, and data sharing to state agencies and institutions of higher education. The Texas Data Literacy Program launched in fiscal year 2023. The Interagency Data Transparency Commission report (2016), required by [SB 1844](#), recommended a formal training and education data literacy program to address enterprise information management, open data, and data sharing practices and protocols.
- **Managing DIR's internal data program.** The OCDO is tasked with managing DIR's internal data program. Led by the officially designated DIR Data Officer, as required

by statute,²²⁶ the DIR data program establishes and coordinates the DIR Data Governance Program, which includes identifying the agency's data assets, exercising authority and management over those assets, and establishing related processes and procedures. The OCDO also manages DIR's records retention schedule and internal DIR policies regarding records management; The DIR Data Officer operationalizes data governance across all DIR programs, including the origination of a data governance policy and a strategy for how to build out the program moving forward.

c) What information can you provide that shows the effectiveness and efficiency of this program or function? If applicable, reference but do not repeat any performance measures from Section II, Exhibit 2, and provide any other metrics of program effectiveness and efficiency. Also, please provide the calculation or methodology behind each statistic or performance measure.

The OCDO does not have budgeted performance measures; however, OCDO does monitor several other metrics:

Figure 58 OCDO Metrics

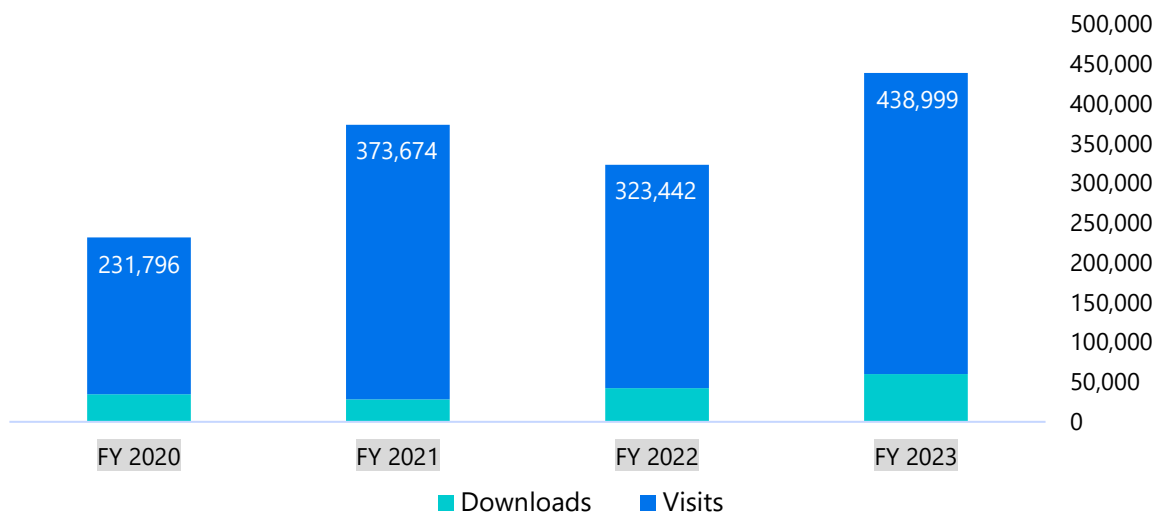
Activity	Metric	Calculation	FY22	FY23
OCDO Briefings, Workgroups, and Focus Groups conducted	Measure of OCDO's hosting of briefings, workgroups, and focus groups that benefit agencies by addressing data and technology issues.	Manual count of hosted briefings, workgroups, and focus groups conducted by OCDO	118	113
Texas Open Data Portal	Number of publishing agencies	Number of agencies publicly publishing on the Open Data Portal	27	35
Texas Open Data Portal	Number of publicly published data assets	Number of assets that are publicly published on the Open Data Portal	644	868
Texas Open Data Portal	Number of visits	Number of visits to Open Data Portal assets, cumulative over the lifetime of the assets	1,230,796	1,806,148
Texas Open Data Portal	Number of downloads	Number of downloads Open Data Portal assets, cumulative over the lifetime of the assets	299,551	391,232
Texas Open Data Portal	Number of ODPUG meetings	Quarterly Open Data Portal User Group (ODPUG) meetings provide education and collaboration opportunities for current and	4	4

²²⁶ [Gov't Code § 2054.0286.](#)

Activity	Metric	Calculation	FY22	FY23
		potential customers of the Open Data Portal		
Texas Open Data Portal	Number of Executive Dashboards	Executive dashboards are created by the Open Data Portal Administrator for the leadership of publishing agencies, to provide insight into their data's usage	13	16
Data Sharing	Number of agencies participating in Texas Statewide Data Exchange Compact (TSDEC) program	Agencies who have signed the TSDEC	21	23
Data Management	Number of Data Management Officers (DMOs) designated	Number of Agencies above 150 FTE that have designated a DMO	64	101
Data Management	Number of Data Management Advisory Committee (DMAC) meetings	Number of quarterly DMAC meetings facilitated by the OCDO	4	8
Texas Data Literacy Program (TDLP)	Number of organizations participating in the eLearning program	Number of state agencies and institutions of higher education participating in the eLearning program	N/A (TDLP launched in FY23)	34
Texas Data Literacy Program	Number of Individuals participating in the eLearning program	Number of individuals participating in the eLearning program	N/A	60
Texas Data Literacy Program	Number of YouTube views	Number of YouTube views per course	N/A	1,320

Open Data Portal Usage by Fiscal Year

Figure 59 Open Data Portal Usage by Fiscal Year



d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

All major functions and responsibilities of the OCDO were created by legislation and have expanded progressively over the past five years.

2015

In 2015, two different bills from the 84th Legislature, Regular Session, impacted data management in Texas: [House Bill 1912](#) and [Senate Bill 1844](#).

[HB 1912](#) created the Statewide Data Coordinator position at DIR to collaboratively develop data policies, standards, and best practices, and improve data governance and integrity statewide.²²⁷

[SB 1844](#) created the Interagency Data Transparency Commission to study and review the current public data structure, classification, sharing, and reporting protocols for state agencies.²²⁸

2016

In 2016, the Interagency Data Transparency Commission released a report based on its review with recommendations for: developing data management programs within state agencies; designating the Open Data Portal as the central repository for open data; and improving interagency data sharing.

2019

In 2019, [SB 819](#) of the 86th Legislature, Regular Session, removed the statewide data coordinator position and in its place established the position of the Chief Data Officer for the State of Texas. Additionally, the bill designated the Open Data Portal as the official central repository for publicly accessible electronic data.²²⁹

2021

In 2021, [SB 475](#) of the 87th Legislature, Regular Session, directed agencies to post a minimum of three high-value data sets on the Open Data Portal; mandated the creation of the Data Management Advisory Committee; and directed agencies with 150 or more full-time

²²⁷ [Acts 2015, 84th Leg., R.S., ch. 1047 \(H.B. 1912\), 2015 Tex. Gen. Laws 3663 \(codified at relevant sections of Government Code Chapter 2054\).](#)

²²⁸ [Acts 2015, 84th Leg., R.S., ch. 639 \(H.B. 1844\), 2015 Tex. Gen. Laws 2076 \(codified at Gov't Code Chapter 2060\).](#)

²²⁹ [Acts 2019, 86th Leg., R.S., ch. 604 \(S.B. 819\), 2019 Tex. Gen. Laws 1772.](#)

employees to designate a Data Management Officer. Data Management Officers are responsible for coordinating with the Chief Data Officer to improve the control and security of information collected by state agencies, promote the sharing of information between state agencies (including customer information), reduce information collection costs, and assist in the development and management of the Texas Data Portals.²³⁰

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The following entities are eligible for services DIR provides, including programs within the Data Management function:²³¹

- State agencies;
- Local government organizations;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Tax Code Section 152.001; and
- Government entities of another state.

State agencies and institutions of higher education with more than 150 full-time employees must designate a Data Management Officer.²³² Data Management Officers cooperate with the

²³⁰ [Acts 2021, 87th Leg., R.S., ch. 567 \(S.B. 475\)](#)(codified at relevant sections of the Government Code).

²³¹ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

²³² [Gov't Code § 2054.137\(a\)](#).

Chief Data Officer to ensure that their agency adheres to that statutory requirement.²³³ As of June 2023, the OCDO identifies 42 state agencies and 62 institutions of higher education with an FTE count above the 150-employee threshold.

State agencies and institutions of higher education with more than 150 FTEs must publish a minimum of three high-value datasets on the Open Data Portal.²³⁴

f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.

Data Management Administration

The OCDO is administered by the Chief Data Officer who oversees the Data Strategy and Implementation Team and the Program Data Analysis and Reporting Team. The Data Strategy and Implementation Team includes the DIR Data Management Officer, the Data Sharing Strategist, and a Data Analyst, and the Program Data Analysis and Reporting Team includes two Data Analysts, a Senior Business Analyst, and the Data Literacy Program Administrator. The primary goals of the OCDO are to improve data governance and integrity statewide; seek opportunities for data sharing across government; and work with agencies and institutions of higher education to collaboratively develop data policies, standards, and best practices.

DIR Data Governance Program

The DIR Data Management Officer administers DIR's internal data governance program, which involves identifying the agency's data assets and implementing best practices and establishing procedures to manage, oversee, and secure these data assets.

Data Management Advisory Committee

The OCDO shares the administrative responsibilities of facilitating the Data Management Advisory Committee. The Chief Data Officer is responsible for the planning and facilitation of the Data Management Advisory Committee meetings. The Chief Data Officer and OCDO team members jointly prepare the meeting agenda, disseminating relevant meeting materials to participants, and encouraging the active engagement of all committee members. Individual Data Management Advisory Committee members are expected to actively engage in meetings, offer insights, and collaboratively participate in decision-making processes. The Chief Data Officer then reports on any insights, best practices, and guidance gleaned from the advisory committee meetings to the DIR Board during the OCDO update at the quarterly open meeting.

²³³ [Gov't Code § 2054.0286.](#)

²³⁴ [Gov't Code § 2054.137\(c\).](#)

The Texas Open Data Portal and Closed Data Portal Program

The Texas Open Data Portal and Closed Data Portal program are managed by the Data Sharing Strategist, who is responsible for the daily operations of the Open Data Portal and supporting existing and onboarding new Open Data Portal customers. The Data Sharing Strategist works with DIR customers in the design, setup, and onboarding of Closed Data Portal instances, which are separate and private data sharing environments intended to host private or sensitive data. Unlike the Open Data Portal in which the data is publicly available without authentication, access to data in the Closed Data Portal is by invitation only. The Data Sharing Strategist also develops educational resources for publishing agencies and leads quarterly Open Data Portal User Group meetings.

Texas Data Literacy Program

The Texas Data Literacy Program is administered by the Texas Data Literacy Program Administrator and provides guidance, training, and education on topics related to data management, open data, and data sharing. To determine priority topics, Data Management Officers and other data professionals from Texas state agencies and institutions of higher education complete an annual data literacy assessment. Data Management Officers and members of an interagency data literacy workgroup contribute to course content and development.

The Texas Data Literacy Program provides eLearning courses on a learning management system platform that are available to Data Management Officers and other staff working on their organization's data management programs. Individuals interested in accessing the platform submit a request to DIR and the Texas Data Literacy Program Administrator completes the registration process to issue a license to the individual. Monthly participation reports are used to monitor platform use and to collect course evaluations.

To make data literacy course content available to a wider audience, video-only versions of the courses are published to the DIR YouTube channel under the Texas Data Literacy Program playlist. Further, the OCDO works with interested state agencies and institutions of higher education to host DIR-created courses on their own learning management system platforms.

Data Sharing

The Texas Statewide Data Exchange Compact is a uniform data sharing and data security agreement for participating Texas state agencies and institutions of higher education. The Texas Statewide Data Exchange Compact contains the standard terms and conditions applicable to all agencies interested in data sharing and exchange. Once executed by all parties, the Texas Statewide Data Exchange Compact enables a more efficient and effective process for sharing data between participating entities.

The OCDO process establishes a common understanding of the use of the Texas Statewide Data Exchange Compact and outlines the responsibilities of the OCDO in Texas Statewide Data Exchange Compact processing and administration, including the Chief Data Officer as the signatory administrator and the Data Sharing Strategist in managing the process of adding

newly signed Texas Statewide Data Exchange Compact documents to the appropriate DIR webpage.

Program Data Analysis and Reporting

The Program Data Analysts and Reporting team provides quality assurance support to DIR programs and provides analysis and data as needed. This team is led by the Senior Business Analyst, who provides procurement support and project management work across multiple business lines and includes two Business Analysts and three management analysts.

The team monitors compliance on vendor sales reports and reviews for accuracy and timeliness. The vendor sales reports are then used to determine how much vendors owe in administrative fees as negotiated in their contracts, which is also monitored for compliance. The Program Data Analysis and Reporting team also conducts market research for procurements and assists in IT application development that supports DIR.

Data Management Processes

The data management processes to facilitate these activities include: orientation for new Data Management Officers; facilitation of Data Management Advisory Committee meetings, Data Advisory Group meetings, and Open Data Portal User Group meetings; the onboarding of customers for the Open Data Portal; the tracking of Open Data Portal changes; the onboarding and registration of eligible staff for the Texas Data Literacy Program; the monitoring and reporting of Texas Data Literacy Program participation; and the administration of the Texas Statewide Data Exchange Compact.

Orientation for New Data Management Officers

When a state agency designates a Data Management Officer, the OCDO grants access to helpful resources. The process for granting new Data Management Officers access to resources includes:

1. The Data Sharing Strategist sends a welcome packet;
2. The OCDO grants access to the OCDO resource SharePoint site; and
3. The OCDO sends invitations to the quarterly Data Management Advisory Committee; and Open Data Portal User Group meetings.

Facilitating Data Management Advisory Committee Meetings

The quarterly Data Management Advisory Committee meetings are comprised of designated Data Management Officers from state agencies and institutions of higher education in addition to the Chief Data Officer.²³⁵ During these meetings, advisory committee members aim to ensure effective communication, collaboration, and decision-making while also aligning with the state's data management goals and objectives and maintaining compliance with relevant

²³⁵ [Gov't Code § 2054.0332](#).

regulations and standards.

The high-level process involves the OCDO coordinating, planning, and facilitating the advisory committee meetings by:

1. Planning for a Data Management Advisory Committee meeting;
2. Scheduling the meeting;
3. Preparing the agenda;
4. Developing relevant reports, presentations, and materials for the meeting;
5. Facilitating the meeting;
6. Recording meeting minutes; and
7. Following up on action items.

Facilitating Data Advisory Group Meetings

The Data Advisory Group is a cross-functional group comprised of the DIR Data Management Officer, Enterprise Data Architect, Information Security Officer, program area leadership, business data stewards, technical data stewards, and IT leadership. The Data Advisory Group supports projects and initiatives by working with stakeholders to prioritize business goals surrounding data and add data governance rigor.

The high-level process involves the OCDO coordinating, planning, and facilitating by:

1. Convening the Data Advisory Group;
2. Collaborating with executive management and IT leadership;
3. Facilitating the identification of business and technical objectives;
4. Assisting with validating and prioritizing work; and
5. Maintaining records and reports on progress.

Onboarding Customers for the Open Data Portal

New DIR customers are provided educational and training materials to support Open Data Portal publishing tasks. The Data Sharing Strategist follows onboarding procedures to ensure that DIR customers have the knowledge and support needed to publish on the Open Data Portal. As interactions with Open Data Portal customers involve a concierge approach, the OCDO procedures may be altered from these onboarding steps to address unique customer needs including welcome information, account creation, metadata additions, education opportunities, and ongoing support.

The Open Data Portal customer onboarding process is outlined in the below chart.

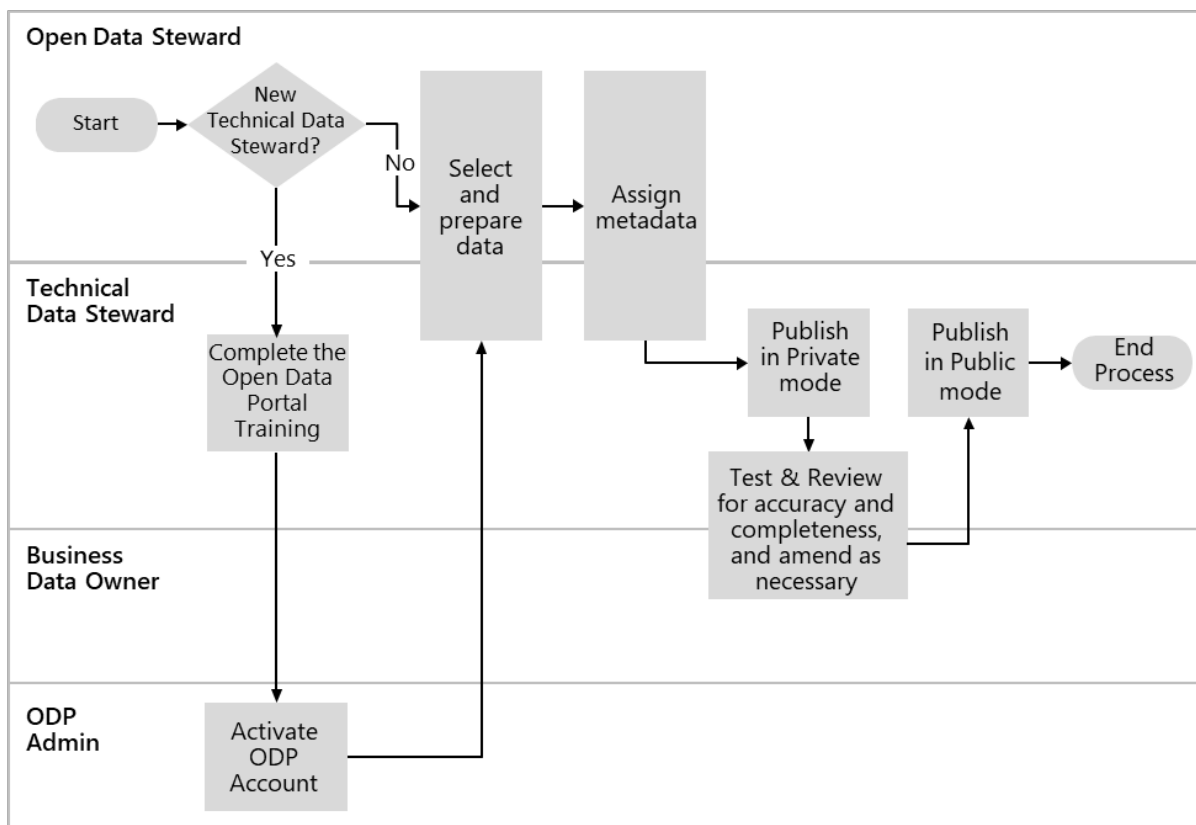
Figure 60 Open Data Portal Onboard Process



The process for posting data to the Open Data Portal is outlined below.

Figure 61 Open Data Portal Posting Process

Publishing ODP Assets Process



Tracking Open Data Portal Changes

To ensure that changes are requested by an appropriate Open Data Portal contact at the requesting agency and that changes are completed in a timely manner according to the request, the Data Sharing Strategist tracks all requested actions including changes. This tracking log maintains program continuity and auditability. The OCDO ensures that all Open Data Portal users have the proper access and role and anyone no longer requiring access has their account disabled as necessary and appropriate.

Facilitating Open Data Portal User Group Meetings

The Data Sharing Strategist schedules and facilitates the Open Data Portal User Group, which offers education and networking opportunities for employees of state agencies and institutions of higher education involved in the development of open data management programs and publishing on the Open Data Portal.

Onboarding and Registration for the Texas Data Literacy Program

The Texas Data Literacy Program's onboarding and registration processes provide a structured approach for onboarding, assigning, and managing registration licenses for Data Management Officers and their designated staff to access the Texas Data Literacy Program eLearning series. Steps for onboarding and registering customers into the Texas Data Literacy Program are

outlined below.

An individual requests access to the Texas Data Literacy Program using the Request for Access Form. Once the form is submitted, the Texas Data Literacy Program Administrator transfers the requestor's information to the registration documentation spreadsheet, ensuring the organization name is standardized and the exact same as other staff within that organization. The Texas Data Literacy Program Administrator indicates in the registration documentation spreadsheet if the organization is a state agency or institution of higher education, and if the requestor is on Data Management Advisory Committee or the Data Literacy Workgroup. (These data elements are needed for performance measure calculations.) The Texas Data Literacy Program Administrator sends a new registration welcome email to each new user. The Texas Data Literacy Program Administrator registers each user within the learning management system for the Texas Data Literacy Program.

Monitoring and Reporting for Texas Data Literacy Program Participation

The Texas Data Literacy Program participation and reporting process provides a structured approach for monitoring and acknowledging participation in Texas Data Literacy Program courses. Steps for monitoring and reporting Texas Data Literacy Program participation include:

The Texas Data Literacy Program Administrator downloads the participation report from the learning management platform on the first working day of each month to:

- Monitor for non-usage of distributed licenses;
- Compare the participation report to the registration documentation spreadsheet and note anyone who has not taken a course within 30 days of registration;
- Contact those users to find out if they are having issues accessing the platform and remind them of their agreement to take a course within 30 days of registration or the license will be reassigned;
- Update the registration documentation spreadsheet with the date a follow-up email is sent; and
- For users not taking a course within 60 days of registration, send a request to the vendor to remove the user from the platform, so the license may be reassigned.

The Texas Data Literacy Program Administrator then updates the master participation file and sends out course completion letters for each course. The Texas Data Literacy Program Administrator updates the registration documentation spreadsheet to add the date the letter was sent for each course completed. Quarterly, the Texas Data Literacy Program Administrator conducts analyses and provides updates for Data Management Advisory Committee and DIR Board of Directors meetings.

Administering the Texas Statewide Data Exchange Compact

The Texas Statewide Data Exchange Compact process establishes a common understanding of the use of the Texas Statewide Data Exchange Compact and outlines the responsibilities of the OCDO in Texas Statewide Data Exchange Compact processing and administration. Steps in the Texas Statewide Data Exchange Compact process are outlined below.

- The agency interested in entering into the data sharing agreement downloads the Texas Statewide Data Exchange Compact from the DIR website and the agency head or designee signs the document. The agency then emails the signed Texas Statewide Data Exchange Compact to the DIR Shared Technology Services Contract Office at sharedservicescontractoffice@dir.texas.gov and copies OCDO@dir.texas.gov.
- The Shared Technology Services Contract Office prepares the document and sends it to the Chief Data Officer in DocuSign for countersignature. The Shared Technology Services Contract Office sends the fully executed Texas Statewide Data Exchange Compact back to the initiating agency and to OCDO@dir.texas.gov, and then records the executed agreement.
- The Data Sharing Strategist or their designee submits a web request to the Chief Experience Office to add a copy of the completed document to the DIR website at: <https://dir.texas.gov/office-chief-data-officer/texas-statewide-data-exchange-compact>. In the web request, the Data Sharing Strategist specifies the appropriate naming convention of **DIR-TSDEC-xxx-AGENCY**, where xxx is the next sequential Texas Statewide Data Exchange Compact agreement number and **AGENCY** is the agency acronym.

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The Data Management function is funded by fees collected through DIR's Texas.gov and Cooperative Contracts programs.

Strategy	Method of Finance	Amount
A.1.1 - Statewide Planning and Rules	Clearing Fund	\$479,128

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

The Texas Natural Resources Information System, a division of the Texas Water Development Board, is the geospatial data clearinghouse for Texas. Although also considered open data, the Texas Natural Resources Information System platform specifically hosts complex geographic information system (GIS) data whereas the Texas Open Data Portal is intended only for raw

data published in open standard, tabular format.²³⁶

Some state agencies and institutions of higher education may develop their own data literacy programs for their employees. However, those efforts would likely target their specific organization's data and priorities while the DIR Texas Data Literacy Program has a statewide and strategic focus.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

Representatives of both DIR and the Texas Water Development Board attend each other's workgroups and meetings (such as the Shared Technology Services GIS Solutions group meeting and DIR's Open Data Portal User Group quarterly meeting) to ensure regular communication. DIR and the Texas Water Development Board avoid duplication of efforts due to the nature of the subject matter and capabilities of the platforms managed by the respective agency. Regular communication ensures that these programs do not come into conflict and instead complement each other.

Many state agencies and institutions of higher education have begun to develop data literacy programs within their organizations. To avoid duplication of effort, an interagency workgroup met approximately monthly during FY22 to determine the scope of the Texas Data Literacy Program with plans to continue to meet approximately quarterly to plan future developments for the program. Additionally, OCDO is working with interested organizations to host DIR-created data literacy courses on their own learning management system platforms. This collaboration ensures consistent messaging across organizations for foundational data management information and allows organizations to focus their efforts on creating program content directly relevant to their needs and specifications.

The OCDO coordinates with the Texas State Library and Archives Commission to provide guidance on the intersection between data management, records, and information management, including best practices, common challenges and solutions, and additional resources for further guidance.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

Eligible local, regional, or federal units of government of the Data Management function include:

²³⁶ [Gov't Code § 2054.1265\(c\).](#)

- Local governments, including counties, municipalities, school districts, and junior college districts;²³⁷
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.²³⁸

The Data Management function works with local and federal units of government. Specifically, the Data Sharing Strategist collaborates with cities, counties, and states in the U.S. as well as internationally on open data best practices. This collaboration is in addition to OCDO's statutory work with state agencies and institutions of higher education across Texas.

The State Chief Data Officers Network is a monthly gathering of statewide Chief Data Officers from across the country. During these gatherings, attending statewide Chief Data Officers meet to share best practices and provide support for other states' efforts to utilize data to deliver better outcomes. The State Chief Data Officers Network is facilitated by the Beeck Center at Georgetown University in Washington, D.C.

An interagency data literacy workgroup, composed of 21 state agencies and eight institutions of higher education, met monthly during FY22, and continues to meet quarterly to determine the scope of the Texas Data Literacy Program, develop course content, and discuss best practices for advancing data management, open data, data sharing, and data analytics in Texas.

The quarterly Data Management Advisory Committee meeting is comprised of designated Data Management Officers from various state agencies and institutions of higher education, in addition to the statewide Chief Data Officer.²³⁹ These meetings aim to ensure effective communication, collaboration, and decision-making among the committee members while aligning with the state's data management goals and objectives and maintaining compliance with relevant regulations and standards.

k) If contracted expenditures are made through this program, please provide:

A Short Summary of The General Purpose of Those Contracts Overall

The contracts in this program are primarily used for operating the Texas Open Data Portal and Private (Closed) Data Sharing Portal and for the DIR data literacy eLearning courses.

²³⁷ [Gov't Code § 2054.003\(9\)](#).

²³⁸ [Gov't Code § 2157.068\(j\)](#); *see also* [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\)](#).

²³⁹ [Gov't Code § 2054.0332\(b\)](#).

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent \$30,457 in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 181 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award date was August 2022 for this contract. The funding source was revenue from the Cooperative Contracts program.

The Method Used to Procure Those Contracts

The method used to procure these contracts was a request for quote.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-CPO-5045	Learning Tree International USA Inc	License fee for hosting DIR's Data Literacy e-learning modules on a learning management system, which makes courses available for agencies and Institutions of Higher Education.	\$30,000.00

The Methods Used to Ensure Accountability for Funding and Performance

DIR's contract and vendor management processes ensure that contractors perform in accordance with all contractual requirements. Active management of service level agreements also ensures that vendors deliver in accordance with each contract.

A Short Description of Any Current Contracting Problems

Not applicable.

I) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

The OCDO is viewed by DIR's customers as the authority and resource to support state agencies and institutions of higher education in their data management journey and develop innovative solutions for data management in Texas. A moderate challenge for the OCDO division is continuing to manage the growth and maturity of the Statewide Data Program to support DIR's customers while undertaking new projects and initiatives such as developing guidance and best practices on data analytics, emergent tools, and technologies.

The OCDO collaborates with other divisions and departments within DIR to optimize the data from DIR-source transactional systems and move that data to a data warehouse to provide a

single source of truth, which will enable report development and self-service reporting. Current challenges include disparate source systems; unclean data; lack of an automated data pipeline to move the data in a reliable and timely fashion; limited data modeling for self-service reporting; and a lack of resources to perform in-depth data analysis and data analytics. A vendor has been awarded to assist with implementing tools, technologies, and processes to help mitigate these challenges.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

Within the agency, the DIR Data Officer collaborates with the Office of the Chief Information Security Officer and DIR's Privacy Officer in the Office of General Counsel to discuss data, information security, records management, and data privacy (including data classification). This collaboration includes developing and updating agency policies and procedures, disseminating information, and providing guidance to staff.

Find out more about the Texas Open Data Portal on DIR's YouTube channel:
<https://youtu.be/OdZXI87VBn4>.

o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility). For each regulatory program, if applicable, describe:

DIR monitors compliance with the following requirements related to the Data Management function.

Designating a Data Management Officer

Why the Regulation Is Needed

Each agency employing more than 150 full-time employees is required to designate a full-time employee to serve as a Data Management Officer.²⁴⁰ This mandate underscores the significance of data management, governance, and transparency within state agencies and institutions of higher education. Designating a Data Management Officer provides a point of contact and advocate for organizational data management initiatives that foster enhanced control over data quality, compliance, and security within the organization. A dedicated Data Management Officer ensures that data is aligned with legal and operational requirements. This alignment aids in enhancing decision-making processes and preserving public trust.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

The OCDO monitors compliance with the statutory requirement. It extends support to newly appointed Data Management Officers by offering useful resources and invitations to the

²⁴⁰ [Gov't Code § 2054.137\(a\)](#).

quarterly Data Management Advisory Committee meetings, facilitated by the Chief Data Officer. Additionally, the Office maintains a list of agencies and institutions of higher education that have 150 or more full-time employees, specifically identifying those that have not yet designated a DMO.

Follow-up Activities Conducted When Non-compliance Is Identified

For state agencies or institution of higher education that have not yet designated a Data Management Officer, OCDO contacts that organization's Information Resources Manager, recognizing that not all Data Management Officers reside in the IT department, to inquire about the identity of the potential individual and the expected time frame for designation.

Actions Available to the Agency to Ensure Compliance

The OCDO follows up with organizations that have not yet designated a Data Management Officer to inquire about the expected time frame for designation. OCDO does not publish a designated Data Management Officer compliance report. DIR is not granted statutory authority to require a state agency or institution of higher education to designate a Data Management Officer.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Publishing High-Value Data Sets

Why the Regulation Is Needed

The Data Management Officer for each agency is required to post at least three high-value data sets on the Texas Open Data Portal.²⁴¹ This approach highlights a commitment to transparency, accessibility, and accountability within government entities, offering insights to constituents and various interested parties on the inner workings and decision-making within the government. By making high-value data assets available, it encourages more nuanced decision-making among lawmakers, businesses, and researchers, while also paving the way for innovative opportunities through the provision of essential information. This requirement, backed by hands-on support, aligns all involved agencies with a unified plan for open data handling and dissemination, fostering consistency.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

The Data Sharing Strategist monitors eligible agencies that have not yet published the required data sets and provides support to those agencies still in need of publishing at least three high-value data sets.

²⁴¹ [Gov't Code § 2054.137\(c\)](#).

Follow-up Activities Conducted When Non-Compliance Is Identified

For agencies or institutions of higher education that have not yet published the required data sets, the Data Sharing Strategist contacts the organization's data set publisher to inquire about their anticipated publishing schedule and offer support.

Actions Available to the Agency to Ensure Compliance

The Data Sharing Strategist follows up with organizations that have not yet published the required data sets and inquires about the expected time frame for publishing. The Office of the Chief Data Officer does not publish a high-value data set compliance report. DIR is not granted statutory authority to require a state agency or institution of higher education to publish three high-value data sets.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – IT Procurement and Contracting



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and **offering innovative and cost-effective solutions for all levels of government.**

a) Provide the following information at the beginning of each program description.

Name of Program or Function: IT Procurement and Contracting

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Lynn Hodde Blue, Chief Procurement Office

Statutory Citation for Program:

Specific Requirements for DIR

[Government Code Section 656.050 Training in Contract Negotiation for Purchases of Information Resources Technologies](#)

[Government Code Chapter 2054, Information Resources Management Act](#)

[Government Code Chapter 2155, Subchapter A, General Provisions](#)

[Government Code Chapter 2155, Subchapter B, General Purchasing Requirements, Procedures and Programs](#)

[Government Code Chapter 2155, Subchapter I, Multiple Award Contract Schedule,](#)

[Government Code Chapter 2157 Purchasing: Purchase of Automated Information Systems](#)

General Contracting Requirements for State Agencies

[Government Code Chapter 791, Interlocal Cooperation Contracts](#)

[Government Code Chapter 2161, Historically Underutilized Businesses](#)

[Government Code Chapter 2254, Professional Services Procurement Act](#)

[Government Code Chapter 2261, State Contracting Standards and Oversight](#)

[Government Code Chapter 2262, Statewide Contract Management](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.



The objective of DIR's IT Procurement and Contracting function is to operate efficient and forward-thinking purchase and delivery systems for government IT needs.

By combining DIR's expertise with the buying power of the state, DIR can offer Texas entities the IT goods and services they need at discounted prices and with favorable contract terms so they can focus on their mission of serving Texans. DIR is the primary agency tasked by statute with procuring IT commodities and telecommunications services for Texas public entities and DIR uses this responsibility to promote compliance with and utilization of the Historically Underutilized Business (HUB) Program among DIR and DIR's customers.²⁴²

The IT Procurement and Contracting function is also responsible for the solicitation and management of the Shared Technology Services contracts, and the procuring of and contracting for the products and services that DIR as an agency uses to operate.

The IT Procurement and Contracting function's objective is achieved through both statewide and internal procurement and contracting and the HUB Program.

Statewide Procurement and Contract Management

One of the core efforts of DIR's IT Procurement and Contracting function is statewide procurement and contract management. Through these efforts, DIR facilitates vast contracting opportunities with leading technology vendors at highly advantageous prices. DIR establishes terms and conditions for these contracts that follow statutory requirements.²⁴³ Through the Cooperative Contracts program (COOP) and the Shared Technology Services (STS) program, DIR awarded over 200²⁴⁴ contracts a year in the last two fiscal years. In FY22, contracts through

²⁴² [Gov't Code § 2157.068\(c\)](#).

²⁴³ [Gov't Code § 2157.068](#).

²⁴⁴ This number fluctuates each year given the nature of Request for Offers to extend across years. DIR awarded 257 new contracts in FY21 and 234 contracts in FY22.

COOP alone resulted in an estimated savings of \$395 million on IT commodities for state agencies, institutions of higher education, local governments, and other eligible entities.²⁴⁵

The statewide contracts are divided into three main groups:

- Cooperative Contracts: a self-service model that enables state agencies to find IT products and services for their staff to implement within their agencies;²⁴⁶
- Shared Technology Services Contracts (also known as Enterprise Contracts): a DIR-managed model in which agencies of any size access best-in-class IT services and products from contracted service providers;²⁴⁷ and
- Texas Agency Network Contracts (TEX-AN): competitively negotiated contracts for local and long-distance voice services, wireless services, data services, internet services, Voice over Internet Protocol (VoIP) services, and other services to support eligible customers' telecommunications infrastructure.²⁴⁸

Cooperative Contracts

Through COOP, DIR offers master contracts for IT commodities, which include IT products and services, with pre-negotiated, base terms and conditions, and minimum discounts.²⁴⁹ These contracts provide a marketplace that other entities can use to obtain goods and services. By using DIR's Cooperative Contracts, customers are able both to tailor their purchases to meet their needs as well as include more prescriptive requirements, additional legal terms, and any other desired provisions that do not conflict with the terms and conditions of the master contract negotiated by DIR. Entities that purchase off of DIR's Cooperative Contracts receive customized delivery of service while still leveraging DIR's competitively negotiated not-to-exceed pricing, essential legal terms, and other protections provided through DIR's standard contracting practices.

COOP procurements are aimed at ensuring best value offerings for technology products and services that serve the needs of eligible DIR customers.

Shared Technology Services Contracts

State law tasks DIR with reducing duplication, generating efficiencies, and realizing savings for

²⁴⁵ In FY22, entities eligible for the Cooperative Contracts program included: state agencies, local governments, institutions of higher education, assistance organizations, out-of-state government entities, Electric Reliability Council of Texas, Lower Colorado River Authority, volunteer fire departments, private schools and private or independent institutions of higher education, and hospital and public safety entities.

²⁴⁶ [Gov't Code § 2157.068](#).

²⁴⁷ Gov't Code Chapter 2054, Subchapters [J](#), [L](#), [O](#).

²⁴⁸ [Gov't Code Chapter 2170](#).

²⁴⁹ [Gov't Code § 2157.068\(b\)](#).

Texans by sharing technology infrastructure, services, and contracts among eligible entities.²⁵⁰ To accomplish this, DIR offers statewide contracts through STS for the Application Services Center, Data Center Services, Managed Security Services, Texas Open Data Portal, and Texas.gov. These programs are described in detail in Section VII. Guide to Agency Programs - Shared Technology Services.

Texas Agency Network Contracts

DIR addresses the procurement and contract management of the state's consolidated telecommunications needs through Texas Agency Network (TEX-AN) contracts.²⁵¹ The TEX-AN contracts program provides a pre-negotiated set of offerings through which eligible entities may obtain TEX-AN services from DIR or its awarded vendors, dependent upon the service. State agencies are statutorily required to use TEX-AN for telecommunications services, though other public entities may also use TEX-AN contracts.²⁵² DIR uses these contracts to provide communication technology services to state agencies, including managing the Capitol Complex Telephone System (CCTS), which is further discussed in Section VII. Guide to Agency Programs - Communications Technology Services.

By using the TEX-AN contracts, customers can tailor their purchases to meet their needs while also including more prescriptive requirements, additional legal terms, and any other desired provisions that do not conflict with DIR's pre-negotiated terms. Entities that purchase off of TEX-AN contracts receive customized delivery of service while still leveraging DIR's competitively negotiated not-to-exceed pricing, essential legal terms, and other protections provided through DIR's standard contracting practices.

DIR aims to deliver its customers the best service for the best value. In support of this goal, DIR oversees and manages order processing, service level agreements, and billing reconciliations for certain contracted TEX-AN service offerings for statewide customers.

Internal Procurement and Contract Management

Internal agency procurements are for goods or services that DIR utilizes for the benefit of its operations or the management of its own programs. Largely, these are the same types of procurements any state agency undertakes.

Historically Underutilized Business (HUB) Program

DIR's HUB Program provides information and support to the HUB vendor community and monitors the use of HUB technology contracts. DIR's HUB Program is unique when compared to other agency HUB programs because it serves eligible statewide customers as well as

²⁵⁰ [Gov't Code § 2054.001.](#)

²⁵¹ [Gov't Code § 2170.002.](#)

²⁵² [Gov't Code § 2170.051\(c\).](#)

internal customers at DIR.²⁵³ DIR follows the Statewide HUB Program rules²⁵⁴ set by the Texas Comptroller of Public Accounts, which sets annual expenditure goals for state agencies and institutions of higher education by procurement categories. DIR and its contracted vendors make a good faith effort to meet or exceed these goals and assist HUBs in receiving a portion of the total contract value of all contracts that DIR expects to award in a fiscal year.

Due in part to DIR's efforts to promote the HUB Program and increase the number of HUB vendors, public entities are increasingly spending more with HUB vendors on DIR contracts. For example, HUB spending through COOP increased from more than \$674 million in FY19 to nearly \$1.1 billion in FY22, a record in Texas. HUB spending in the Shared Technology Services Program increased from nearly \$20 million in FY19 to \$33 million in FY22.

The IT Procurement and Contracting function's major activities fall under three categories:

- IT Procurement;
- IT Contract Management; and
- Historically Underutilized Business Program Management.

IT Procurement

To procure IT products and services, DIR uses competitive procurements to solicit responses from vendors and obtain the best value for the state. Major activities include:

- Establishing master contracts for IT products and services that both DIR and DIR's eligible customers may use.
- Developing and overseeing the entire lifecycle of solicitations, including gathering customer input and requirements; drafting and posting the solicitation; evaluating the responses; negotiating pricing, terms, and conditions; and awarding the contracts.
- Collaborating with DIR staff across DIR's programmatic areas on procurements.
- Advising customers on procurement strategies; providing consultative services and training required for state certified procurement professionals; and facilitating statutorily required technology negotiations training and vendor training.

IT Contract Management

At any given time, DIR manages approximately 800 contracts with 3,000 vendors offering tens of thousands of products from over 2,800 brands. Major activities include:

- Monitoring contract and vendor performance, conducting contract compliance reviews, reviewing invoices and deliverables, and resolving issues for customers.

²⁵³ [Gov't Code § 2157.068\(c\).](#)

²⁵⁴ [34 Tex. Admin. Code Chapter 20.](#)

- Reviewing state agency statements of work (SOWs) that are valued at more than \$50,000 to ensure their inclusion of statutorily required terms and consistency with DIR's master contract language.²⁵⁵
- Considering state agency exemption requests to purchase technology-related items valued at more than \$10,000 from a vendor who has not been awarded a cooperative contract or a product or service that is not available through a cooperative contract.²⁵⁶
- Negotiating bulk purchase agreements to leverage the bulk buying power of Texas,²⁵⁷ which saves state and local governments – and more importantly, taxpayers – millions of dollars each year.

Historically Underutilized Business Program Management

DIR's HUB Program provides information, training, and support to the HUB vendor community and monitors the use of HUB technology contracts as reported by awarded vendors. The Historically Underutilized Business Program Management function's major activities include:

- Monitoring HUB compliance and contract performance across all program areas.
- Providing guidance on HUB Program requirements and compliance, including reviewing vendors' HUB Subcontracting Plans for compliance with DIR's HUB goals prior to the submission of the RFO.
- Offering HUB-specific trainings designed to increase awareness of the statewide HUB Program and educate the vendor community regarding HUB compliance.
- Educating the HUB vendor community about the HUB Program and how to work with DIR.
- Attending HUB outreach events, such as spot bid fairs and conferences.

c) What information can you provide that shows the effectiveness and efficiency of this program or function? If applicable, reference but do not repeat any performance measures from Section II, Exhibit 2, and provide any other metrics of program effectiveness and efficiency. Also, please provide the calculation or methodology behind each statistic or performance measure.

DIR monitors the effectiveness and efficiency of the IT Procurement and Contracting function through various metrics, such as sales and cost avoidance tracking, service level agreement measurement, and customer satisfaction scoring.

²⁵⁵ [Gov't Code § 2157.0685](#); see also [1 Tex. Admin. Code § 212.41](#).

²⁵⁶ [Gov't Code § 2157.068\(f\)](#); see also [1 Tex. Admin. Code § 212.20](#).

²⁵⁷ [Gov't Code §§ 2157.068\(a\), \(e-3\)](#).

IT Procurement and Contract Management

Cooperative Contracts

DIR monitors approximately 800 Cooperative Contracts²⁵⁸ that result in savings to the state through economies of scale and reduced administrative costs. Public entity purchases through COOP exceeded \$3 billion during FY22, a 50 percent increase in just four years. In that same time, DIR saved more than 3,900 Texas government entities and Texas taxpayers approximately \$1.4 billion.

Additionally, since 2019, out-of-state utilization of COOP increased by more than 129 percent, including more than 576 out-of-state government entities from 44 other states.

Figure 62 Cooperative Contract Sales (FY22)

Customer Channel	Sales (in \$ Millions)	Cost Avoidance (in \$ Millions)
Education (K-12)	\$891.6	\$127.5
Local Government	\$783.4	\$97.2
State Agencies	\$839.6	\$95.4
Higher Education	\$446.8	\$60.7
Out-of-State Government	\$84.6	\$13.2
Assistance Organizations	\$4.7	\$1.0
Total	\$3,050.6	\$395.0

Shared Technology Services Contracts

The efficiency and effectiveness of the STS Contracts is measured by vendor performance and customer satisfaction, the results of which are provided in Section VII. Guide to Agency Programs – Shared Technology Services.

In 2020, DIR greatly expanded the Shared Technology Services offerings when the DIR Board approved the award of six new Next Generation Data Center Services contracts. Through these procurement efforts, DIR seized the opportunity to negotiate the core services' rates below pricing in prior contracts.

DIR's reinvestment strategy enabled the addition of the following to the Shared Technology Services:

- Customer relationship management, expanded security tools, and an expanded service management toolset for the Multi-sourcing Services Integrator (MSI) that further enhanced the abilities of the program;

²⁵⁸ This number fluctuates at any given time based on contract cycles and terms.

- Independent third-party solutioning services, which brought oversight to infrastructure and solutioning in the public and private clouds;
- Strategy management services to include technology planning, evolution, roadmaps, and the creation of a new service to provide dedicated customer technical architects to assist agencies in legacy modernization; and
- Next generation technology solutions, enhanced cybersecurity tools and services, and the creation of a public cloud center of excellence (Cloud CoE).

Texas Agency Network Contracts

TEX-AN Contracts are procured through the request for offer process, during which DIR negotiates with telecom vendors who submit a response for consideration for firm-fixed pricing of services.

Each TEX-AN Contract contains negotiated pricing by service, allowing customers to compare vendor contract pricing across all TEX-AN vendors. Contracts also include management plans related to the services offered, service level agreements, and order processing. In addition to administering the order process, service level agreements, and billing reconciliation for these contracts, DIR establishes the management plans to ensure that all customers are treated equally, regardless of size.

DIR establishes firm-fixed pricing for all customers creating a multi-vendor environment where vendors compete for customers and can see each other's prices. Additionally, as prices are lowered, both current and new customers enjoy savings. Customers can compare pricing directly from multiple contracts all in one place rather than trying to validate a discount off the manufacturer's suggested retail price. When DIR's customers are not subject to separate pricing schedules, the billing and reconciliation processes are more effective and efficient for state government.

Bulk Purchase Agreements

Article IX, Rider 9.04, "Information Technology Replacement," in the General Appropriations Act (87th Legislature)²⁵⁹ requires agencies and institutions of higher education to participate in hardware and software bulk purchasing efforts facilitated by DIR, when appropriate. DIR coordinates bulk purchasing agreements when at least two or more eligible customers have requested to buy a product.²⁶⁰ Bulk purchasing agreements allow DIR to leverage the purchasing power of the state to obtain best value for customers intending to purchase in bulk where multiple customers have expressed interest in the same IT commodity.

In addition to state agencies and institutions of higher education, other eligible entities may purchase through these agreements, including local governments, assistance organizations as

²⁵⁹ [General Appropriations Act, 88th Leg., R.S., ch. 1170 \(H.B.1\).](#)

²⁶⁰ [Gov't Code §§ 2157.068\(a\), \(e-3\).](#)

defined by [Government Code Section 2175.001\(1\)](#), and out-of-state public entities.

In FY21 and FY22, by using the DIR Cooperative Contracts for bulk purchases, DIR successfully achieved its goal of maximizing Texas' cost savings by leveraging agencies' combined need for these products and solutions to reduce purchasing costs while increasing options to meet individual agency technology requirements. The bulk purchasing efforts saved participating state agencies more than \$17 million based on data captured by the DIR Vendor Sales Reporting (VSR) Portal. Overall, in FY19 and FY20, 199 eligible customers purchased nearly \$54 million in bulk purchases, resulting in a savings of more than \$21 million. Overall, in FY21 and FY22, there were 32 customers that purchased over \$54.9 million through the bulk purchase contracts with over \$18 million in savings.

Figure 63 Purchases and Savings by Customer Segment for FY21 and FY22

Customer Segment	Number Participating	Purchases	Savings
Higher Ed	2	\$346,526	\$399,825
Local Government	5	\$552,641	\$515,500
State Agencies	25	\$54,039,106	\$17,086,957
Total	32	\$54,938,273	\$18,002,282

Historically Underutilized Business Program Management

DIR consistently exceeds the statewide goals established by the Texas Comptroller of Public Accounts for HUB spend in business categories tracked by the state, including professional services, other services, and commodity purchases. In FY22, DIR achieved 33 percent in the category of "other services," which exceeded DIR's HUB goal of 26 percent. In the "commodities" category DIR achieved 19 percent of DIR's established HUB goal of 21.1 percent.

At a statewide level, customers purchased more than \$1 billion from HUB vendors through the COOP program in FY22.

DIR also provides many kinds of HUB-related trainings, including training:

- Required for state-certified procurement professionals;
- On technology negotiations that are statutorily required;
- For vendors; and
- That is HUB-specific and designed to increase awareness of the statewide HUB Program in addition to educating the vendor community regarding HUB compliance.

DIR also attends outreach events, such as spot bid fairs and conferences, to educate vendors about working with DIR. DIR increased its procurement and contracting related training and outreach events by 28.8 percent in FY22 from FY21, as reflected in the chart below.

Figure 64 DIR HUB Outreach and Training Events

Fiscal Year	Count of Events
2021	165
2022	232

DIR's outreach efforts are helping to increase HUB vendors' responses to DIR procurement opportunities.

In addition, HUB Subcontracting Plan reviews went up from 1,569 to 1,841, an increase of 14.7 percent from FY21 to FY22, which indicates that DIR is awarding more contracts with HUB subcontractors and HUB resellers.

d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

2008

Sales through DIR's Cooperative Contracts program exceeded a billion dollars for the first time in the program's history, reflecting its extensive use by customers across the state and nation.

2015

DIR's IT Procurement and Contracting function and responsibilities matured significantly beginning with the passage of [Senate Bill 20](#) (84th Legislature).²⁶¹ Through [SB 20](#) and subsequent legislation, DIR assumed additional responsibilities, including providing training to state agency staff engaged in IT negotiations, reviewing and approving agency statements of work, and implementing appropriate internal contracting controls to be compliant with revised statutes, rules, and guidelines.²⁶²

2016

DIR aligned agency procurement and contracting functions under the newly established Chief Procurement Office (CPO), a rebranding from its previous role as the Technology Sourcing Office. This marked the beginning of DIR's alignment of its procurement and contracting functions and staff to support the expanding STS offerings available to eligible customers through STS (as further described in VII. Guide to Agency Programs – Shared Technology Services).

²⁶¹ [Acts 2015, 84th Leg. R.S., ch. 326 \(S.B. 20\), §§ 15 - 16, 18, 2015 Tex. Sess. Law Serv. 1477 \(codified at various sections of Gov't Code\).](#)

²⁶² [Id.](#)

2017

The Legislature increased DIR's COOP purchasing thresholds from \$1 million to \$5 million in [SB 533](#).²⁶³

DIR launched the BidStamp Vendor Information System, which allowed technology vendors to electronically submit their responses to DIR for cooperative contract procurements. The BidStamp Vendor Information System positively impacts the Cooperative Contracts program by allowing more vendors to submit responses electronically, removing traditional barriers to mailing-in and hand delivering solicitation proposals.

2020

In response to the global COVID-19 pandemic, DIR negotiated and published [bulk purchasing agreements](#) that assisted Texas government's accelerated shift to a remote workforce. This shift to remote work required DIR to support customer sourcing and acquisition of laptops, headsets, mobile phones, hardware, software, and services in response to the COVID-19 disaster. Customer purchases through agreements and other Cooperative Contracts during the first year of the pandemic totaled approximately \$12 million.

As consumption of DIR products and services increased and DIR expanded its COOP and STS offerings, DIR recognized the need to achieve excellence in procurement and contracting to support both DIR and its growing customer base. To this end, DIR transformed the organizational structure of its CPO in anticipation of strengthening its procurement and contracting focuses and core competencies. CPO combined and further aligned critical procurement and contracting functions to industry-standard guidelines and the State Procurement and Contract Management Guide.

2021

The 87th Legislature increased DIR COOP purchasing thresholds to \$10 million through [SB 799](#).²⁶⁴

2022

Sales through DIR's Cooperative Contracts program reached over \$3 billion, resulting in approximately \$395 million in savings to Texas public entities.

DIR set a record for DIR HUB purchases made through the Cooperative Contracts program with \$1.1 billion in purchases.

²⁶³ [Acts 2017, 85th Leg., R.S., ch. 556 \(S.B. 533\), § 8, 2017 Tex. Sess. Law Serv. 1532, 1535 \(codified as an amendment to Gov't Code § 2157.068\).](#)

²⁶⁴ [Acts 2021, 87th Leg., R.S., ch. 855 \(S.B. 799\), § 11 \(codified as an amendment to Gov't Code § 2157.068\).](#)

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The following entities are eligible for DIR services, including programs within the IT Procurement and Contracting function:²⁶⁵

- State agencies;
- Local government organizations;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Tax Code Section 152.001; and
- Government entities of another state.

In FY22, 3,433 different customers used the Cooperative Contracts program. The below table further elaborates on DIR's IT Procurement and Contracting function customers.

Figure 65 Cooperative Contracts Breakdown by Customer Type

Customer Type	Count	% of Overall Customers	Total Sales	% of Total Sales
Local Government	1,471	42.85%	\$783.4M	25.7%
K-12	1,254	36.53%	\$891.6M	29.2%
Higher Ed	196	5.71%	\$446.8M	14.6%
State Agency	117	3.41%	\$839.6M	27.5%
Out of State	336	9.79%	\$84.6M	2.8%

²⁶⁵ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

Customer Type	Count	% of Overall Customers	Total Sales	% of Total Sales
Assistance Org	59	1.72%	\$4.7M	0.2%
Total	3,433	100%	\$3.05 B	100%

f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.

IT Procurement and Contract Management Administration

DIR's IT Procurement and Contracting function is primarily administered by DIR's Chief Procurement Office (CPO), which is led by the Chief Procurement Officer and the Deputy Chief Procurement Officer. Although employees throughout DIR participate in IT procurement and contract management tasks as needed to support the agency's mission, the teams that administer and are primarily responsible for the IT Procurement and Contracting function include the:

- Cooperative Contracts Procurements team;
- Shared Technology Services Procurements team;
- Cooperative Contracts Management team;
- Shared Technology Services Contracts Management team;
- TEX-AN Contracts Management team;
- Program Data Analysis and Reporting team;
- Internal Procurements and Contracts Management team; and
- HUB Outreach and Training team.

These teams are separated by major activity in this subsection for clarity.

Due to the complexity and scale of the statewide procurements and contracts that DIR manages, DIR implemented a governance model that includes input and decision-making from many DIR programs. The DIR governance model is further described later in this section.

As the Legislature granted DIR the authority to add 39 new FTEs in FY23, the teams within CPO expect to add new positions to support the activities of the IT Procurement and Contracting function.

Statewide IT Procurements

DIR's Chief Procurement Office manages and leads the procurements of statewide technology and technology services contracts and the management of the awarded contracts. The COOP Procurements and Shared Technology Services Procurements teams lead the procurement processes in their respective areas.

Cooperative Contracts Procurements Team

The COOP Procurement team is responsible for Cooperative Contract Program procurements,

with expertise, support, and assistance provided by other relevant DIR staff. In FY22, the COOP Procurements team provided 263²⁶⁶ new contracts through Cooperative Contracts.

The Cooperative Contracts Procurements Director manages nine Procurement Leads and reports to the Deputy Chief Procurement Officer. The Director plans the Cooperative Contracts procurement schedule for the year, assigns individual Cooperative Contracts procurements to the Procurement Leads, and oversees each phase of the procurement to ensure compliance with DIR's procurement plan.

The Procurement Leads:

- Oversee and prepare scope of work, specifications, and terms and conditions for new contracts as assigned by the Cooperative Contracts Procurements Director;
- Coordinate the distribution of bid invitations to vendors;
- Review submitted proposals for administrative compliance;
- Lead negotiations;
- Award new contracts; and
- Ensure compliance with current procurement and contracting policies, regulations, and procedures for the Cooperative Contracts program.

Shared Technology Services Procurements Team

The primary responsibility of the Shared Technology Services Procurements team is the procurement of contracts for services in the STS programs. These procurements are for high-value, IT-managed service contracts and require complex contracting processes to address the detailed, highly technical, and necessary requirements. As such, these procurements must be carefully planned, rigorously executed, and carefully managed by the Shared Technology Services Procurements team with support from employees across DIR, including subject matter experts from the substantive program areas, the Office of General Counsel, and members of executive management. The Shared Technology Services Procurements team also manages TEX-AN procurement tasks.

The secondary responsibility of the Shared Technology Services Procurements team is the procurement of IT commodities within STS, which supports the Application Service Center operations discussed in VII. Guide to Agency Programs – Shared Technology Services. The team oversees and assists customers and vendors as the program procures new IT commodities for STS private or public cloud deployment.

DIR's Shared Technology Services Procurements team, which is also referred to as the Enterprise Procurements team, includes the Director of Enterprise Procurements who manages

²⁶⁶ The number of contracts will fluctuate based on Deliverables-Based IT Services and Information Technology Staff Augmentation Contracts, the highest volume of contract awards through COOP. DIR established 257 contracts in FY21 and 234 contracts in FY22.

a team composed of one Procurement Team Lead, four Procurement Leads, and one STS IT Commodity Procurements Lead.

The Director of Enterprise Procurements oversees Shared Technology Services and TEX-AN procurement phases, works with DIR program areas to plan procurements, and collaborates with the Chief Operations Office to advance the Shared Technology Services procurements.

The Procurement Team Lead directs the team, providing support, mentorship, and guidance to other team members, and serves as backup support to the Director of Enterprise Procurements.

The Procurement Leads coordinate TEX-AN, Shared Technology Services, and IT Commodities procurements, including distributing bid invitations to vendors, reviewing submitted proposals for administrative compliance, leading negotiations, and awarding new contracts. They also consult with customers, evaluate customer requirements, and advise them on developing contract specifications that achieve an optimal balance between best value and cost savings. Additionally, the team conducts customer workgroups to gather input for use in developing RFO specifications and serve as procurement liaisons for customer agencies.

Statewide IT Contracts Management

DIR's Chief Procurement Officer manages and leads statewide contract management. The COOP and STS Contracts teams lead contract management activities for the programs that they oversee. The contract teams collaborate extensively with members of other divisions in DIR, including the Chief Technology Office, Chief Operations Office, and Chief Financial Office, to ensure a holistic viewpoint that informs their contract management tasks.

Cooperative Contracts Management Team

The Cooperative Contracts Management team includes the Contracts Management Office Director, two Contract Administration Manager Team Leads, eight Contract Administration Managers, and four Contract Specialists.

The team is responsible for:

- Managing IT commodities and services Cooperative Contracts, Deliverables-Based IT Services (DBITS), IT Staff Augmentation Contracts (ITSAC), bulk purchase agreements, and exemption requests; and
- In compliance with [1 Texas Administrative Code Chapter 212, Subchapter E](#) and [Government Code Section 2167.068](#), reviewing state agency statements of work (SOWs) valued at more than \$50,000 to ensure their inclusion of statutorily required terms and consistency with DIR's master contract language.

As the COOP program continues to grow, DIR anticipates adding staff to this team as authorized by the 88th Legislature's grant of additional FTEs to DIR.

The Contracts Management Office Director oversees the COOP Contracts Management team and assigns contracts to Contract Administration Managers and Contract Specialists.

The Contracts Administration Managers and Contract Specialists work with the Cooperative Contracts Procurement team on cooperative contract procurements and, following the award of contracts under the solicitation:

- Serve as resources for customers to help find contracts that meet their needs;
- Monitor contract performance to ensure contract compliance, track key metrics and fiscal data, and identify cost savings;
- Process contract documents in alignment with contract and vendor management principles;
- Review contract terms with management to ensure their understanding and receive the appropriate authorization;
- Work with the Office of General Counsel on contract terms, clauses, and other related updates to contract management documents; and
- Process contract extensions, and modifications to include pricing changes, new products or emerging technologies additions, and product deletions.

Shared Technology Services Contracts Management Team

DIR's Shared Technology Services Contracts Management team is composed of one STS Contracts Management Director, who manages one Team Lead and four Contract Managers. This team is generally responsible for performing contract administration management activities for the STS programs. To integrate and manage the services of the service component providers, STS is a multi-vendor model that comprises contracts for service component delivery to include Data Center Services, Application Services Center, Managed Security Services, Texas.gov, the Texas Open Data Portal, and the Multi-sourcing Services Integrator (MSI).

Management of contracts of such size and complexity requires expertise and effort from many diverse program areas. The STS Contract Management team is ultimately responsible for managing these contracts, but various DIR staff support or augment contract management tasks, particularly the Chief Operations Office vendor management teams who are intimately involved with the bulk of both vendor and programmatic performance for the programs. The Chief Operations Office manages much of the day-to-day relationships with the vendors and because of their technical capabilities are able to understand how best to meet customer needs through the product offerings of the contracted vendors. If an employee who is not a member of the Shared Technology Services Contracts Management team is responsible for completing a contract management task, then they must communicate any issues or concerns to the assigned STS Contract Manager.

The STS Contracts Management Director oversees the STS Contracts Management team, participates on governance boards, assigns contracts to the Team Lead and Contract Managers, and works with Contract Managers on deliverable issues. The Team Lead works on specialized projects.

The Team Lead and Contract Managers monitor and process vendor deliverables for timeliness, completeness, and accuracy. They conduct contract compliance reviews and performance analysis, assist in documenting vendor performance issues in support of corrective action plans.

and assist in the monitoring of contractual requirements.

Contract Managers assist in developing and negotiating contract amendments and contract correspondence, ensuring all amendments contain current contract language. They also act as customer service representatives to resolve issues with vendors and contractual issues that arise during the term of the contract.

TEX-AN Contracts Management Team

The TEX-AN Contracts Management team, which is composed of two Contract Administration Managers who report to the Director of DIR Internal Procurements, is responsible for the management of the TEX-AN contracts. The Director of DIR Internal Procurements leads the team.

The Contract Administration Managers coordinate the TEX-AN procurements and contract management by:

- Overseeing and preparing scope of work, specifications, and terms and conditions for new TEX-AN contracts;
- Coordinating the distribution of bid invitations to vendors;
- Reviewing submitted proposals for administrative compliance, leading negotiations, and awarding new TEX-AN contracts;
- Monitoring contract performance, ensuring contract compliance, tracking key metrics and fiscal data, and identifying cost savings;
- Providing guidance and insight to customers and administering contract compliance with the vendors through quarterly vendor performance meetings to discuss services, sales, and contract and operational compliance; and
- Providing customer training as necessary and requested.

Although responsibility for these contract management tasks rests solely with the TEX-AN Contracts Management team, the team collaborates extensively with the Communications Technology Services function in the Chief Operations Office.

Internal Procurements and Contracts Management

While DIR's statewide programs have separate procurement and contract management departments, DIR's internal procurement and contract management functions are managed by a single department. DIR's internal procurement and contract management needs are not as complex or numerous as those managed by the statewide program so DIR is able to derive more efficiency with dual certified staff managing both functions as a single department.

Internal Procurements and Contract Management Team

The DIR Internal Procurements Director oversees the DIR Internal Procurements team, which includes two Procurement Leads and one Purchaser, and the Internal Contract Management Team, which includes DIR Internal Contract Managers.

The DIR Internal Procurements team leads DIR's internal procurement efforts and oversees TEX-

AN contracts. DIR employees across the agency, particularly subject matter experts who will ultimately rely on the goods or services being procured, often assist with internal procurements.

The DIR Internal Procurements Director assists and directs the team on procurements and contracts management.

The Procurement Leads:

- Oversee and prepare scopes of work, specifications, and terms and conditions for new contracts;
- Coordinate the distribution of bid invitations to vendors;
- Review submitted proposals for administrative compliance;
- Lead negotiations; and
- Award new contracts.

Once a contract is awarded, the DIR Internal Procurements Director assigns the contract to an Internal Contract Manager to manage.

The Contract Managers:

- Monitor contract performance, ensure contract compliance, track key metrics and fiscal data, and identify cost savings;
- Consult with customers, evaluate customer requirements, and advise them in developing contract specifications that achieve optimal balance between best value and cost savings;
- Conduct customer workgroups to gather input for developing procurements; and
- Serve as a resource to other CPO staff and agency program areas on escalated issues of an unusual nature.

HUB Program Management

DIR's HUB Program monitors HUB requirements and compliance on all DIR procurements and contract management activities. The HUB Outreach and Training team administers the HUB Program.

HUB Outreach and Training Team

The HUB Program is administered by the HUB Outreach and Training team, which includes the Director of HUB Outreach and Training, who manages one HUB Outreach and Training Team Lead, three HUB Coordinators, and one Outreach and Training Coordinator.

In general, the HUB Outreach and Training team:

- Participates in the planning, execution, and oversight of procurements and contracts across DIR;
- Monitors compliance of contracts of all sizes and complexity;
- Is ultimately responsible for HUB compliance with DIR contracts;
- Coordinates HUB requirements with procurement and contract management teams;

- Confers with the Office of General Counsel and executive leadership on matters of relevance within the HUB Program; and
- Reviews HUB submissions to assist with compliance and increase understanding of working with HUBs.

The Director of HUB Outreach and Training, who is also the Deputy Chief Procurement Officer, oversees the HUB Program and leads the HUB Outreach and Training team.

The HUB Team Lead:

- Serves as a liaison for vendors with DIR divisions and programs, and develops and maintains rapport with non-HUB vendors to encourage possible future subcontracting opportunities;
- Works with DIR divisions to ensure that DIR meets or exceeds its established HUB goals;
- Identifies HUB sources for DIR to use in all procurement methods;
- Works closely with agency purchasing staff to identify HUB vendors for DIR procurement opportunities;
- Assists procurement teams with their development of procurement specifications and HUB Subcontracting Plans;
- Monitors agency procurements to determine areas with low HUB participation and reevaluates existing long-term contracts for HUB participation;
- Coordinates training for the recruitment and retention of HUBs;
- Prepares reports documenting program compliance and progress towards established goals;
- Participates in establishing and monitoring of annual HUB goals;
- Attends and coordinates agency participation in HUB forums, trade shows and minority business association meetings; and
- Informs purchasing staff of HUB forums, trade shows or exhibits that showcase minority and women-owned businesses.

The HUB Coordinators assist in developing and recommending outreach and training program guidelines, policies, and procedures, including the review, revision, and maintenance of policies and procedures as required. Additionally, the HUB Coordinators:

- Analyze and provide input for agency reports, and document program compliance and progress toward established goals;
- Assist minority, women-owned, and service-disabled veteran-owned businesses with the Comptroller of Public Accounts (CPA) Statewide Procurement Division certification process; and
- Maintain close relationships with the minority and women-owned business community.

The Outreach and Training Coordinator plans and presents trainings across the state and acts as a subject matter expert on Cooperative Contracts program, often representing the HUB

Program at conferences and forums networking with vendors and customers. This role reports to the Chief Experience Officer. In addition, this role also:

- Serves as a liaison for the vendor community with agency divisions and programs;
- Develops and maintains rapport with customers and vendors for outreach, training, and education needs;
- Writes, edits, and updates informative materials that describe the agency's Chief Procurement Office program areas;
- Establishes and maintains strong working relationships with vendors and customer; and
- Manages complex interactions involving vendors, customers, and the agency.

The Role of DIR's Governance Model

Because DIR is responsible for many high-value procurements and contracts that deal with highly technical, complex, and rapidly changing fields, DIR relies on a multi-tiered governance model to ensure the integrity of these processes, provide the highest levels of accountability, and maintain the highest quality of decision-making possible.

IT Procurement

For DIR's internal purchases, the Internal Procurements Director identifies the appropriate approach for the solicitation, whether direct acquisition or project-based, and manages the procurement according to each of the procurement cycle stages. This process may encompass a variety of shared and independent activities, based on the procurement and contract type, solicitation method, value, and complexity, among other considerations.

For STS and TEX-AN procurements, CPO complies with the Chief Procurement Office Process Guide.

DIR utilizes a governance and oversight structure that involves two independent teams of senior-level leaders and subject matter experts, known as the Source Selection Authority and the Source Evaluation Board. This structure preserves the integrity of the procurement process and ensures high quality decision-making by leveraging the broader knowledge base, experience, and viewpoints afforded by working in teams.

Source Evaluation Board

The Source Evaluation Board provides strategic direction to the procurement process. The team serves as an oversight body for major projects and reviews and approves draft solicitation materials at all phases of these projects.

The Source Evaluation Board's membership is permanent, rather than being established on an ad-hoc basis, and consists of voting members or advisors from the:

- Chief Procurement Office;
- Chief Operations Office;
- Chief Technology Office;

- Chief Financial Office;
- Office of the Chief Information Security Officer; and
- Office of General Counsel.

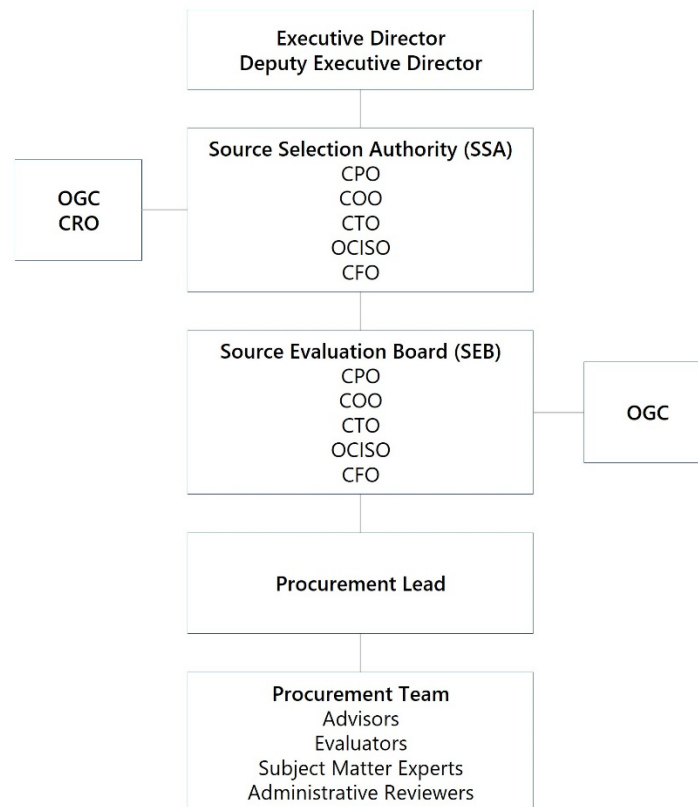
The Source Evaluation Board’s recommendations are reviewed by the Source Selection Authority, which serves as the decision point for board recommendations.

Source Selection Authority

The Source Selection Authority consists of certain executive management. It is responsible for approving solicitation materials for external review and publication, evaluations, and award decisions.

In addition to these duties, the Source Selection Authority serves as decision makers for the Source Evaluation Board’s recommendations. The Executive Director and Deputy Executive Director are non-voting members who participate in the meetings but are only called to cast a vote in the event of a tie amongst other members.

Figure 66 Source Selection Authority



IT Contract Management

DIR’s operational governance framework for the STS programs facilitates coordination between the designated Contract Managers and other parts of the agency. Among other things, this

framework is used to address post-award issues requiring an operation, transition, financial, legal, security, data privacy, or contractual decision. This framework exists for the Texas.gov, Data Center Services (DCS), and Managed Security Services programs, specifically.

Operational Governance Model

The Operational Governance model utilizes two levels of oversight and authority:

- An Operational Governance Board (OGB); and
- An Operational Governance Authority (OGA).

The OGB attempts to obtain consensus from participant stakeholders whenever possible, but defaults to majority vote among the three designated members from the Chief Technology Office (CTO), the Chief Procurement Office (CPO), and the Chief Operations Office (COO) when they cannot reach a consensus.

If the OGB cannot reach a decision by majority vote, then the OGB escalates the issue to the OGA for a decision.

This process is discussed in further detail in Section VII. Guide to Agency Programs - Shared Technology Services.

Procurement, Contracting, and HUB Processes

DIR staff follow a standard procurement cycle for all procurement and contracting activities established through processes set forth in the Chief Procurement Office Process Guide.

Exemptions Processes

As described throughout this document, state agencies are required to procure certain IT goods and services through DIR.²⁶⁷ DIR may, however, exempt a state agency from this requirement for certain purchases.²⁶⁸ DIR must approve an exemption request before an agency awards a technology purchase outside of a DIR contract.²⁶⁹

The following categories generally do not require an exemption:

- The required hardware, software, or technology service is currently offered through a DIR contract; or
- The purchase is for an IT commodity, the value of which is either less than \$10,000 or exceeds \$10 million.²⁷⁰

Generally, a customer may need to file an exemption request because the required product or

²⁶⁷ [Gov't Code § 2157.068](#).

²⁶⁸ *Id.* at §(f); see also [1 Tex. Admin. Code § 212.20](#).

²⁶⁹ [Gov't Code § 2157.068\(i\)\(1\)](#); see also [1 Tex. Admin. Code § 212.20\(a\)-\(b\)](#).

²⁷⁰ 1 Tex. Admin. Code §§ [212.10](#), [212.11](#).

service:²⁷¹

- Cannot be found on a DIR contract;
- Is similar to an option available through DIR's COOP program that does not meet the needs of the agency; or
- Is compatible with the existing technology infrastructure of the agency whereas the products or services available to them through a DIR contract are not.

Blanket Exemptions Processes

To facilitate the exemption process, DIR has established a series of blanket exemptions that state agencies may utilize if the agency determines that the exemption applies to the procurement in question.²⁷² State agencies utilizing these blanket exemptions must maintain a record of the blanket exemption in their procurement file; however, they do not need to submit the blanket exemption to DIR for approval.

DIR maintains ongoing blanket exemptions for:

- Minimum Threshold Procurements: State agencies are granted an exemption from the statutory requirement to purchase IT commodities through a DIR contract for procurements that are less than \$10,000.
- Maximum Threshold Procurements: State agencies are granted an exemption from the requirement to purchase through a DIR contract when purchasing IT commodities²⁷³ in which the value of the contract exceeds \$10 million.²⁷⁴ For a contract with a value between \$5 million and \$10 million, a state agency may purchase an IT commodity using a purchasing method designated by the Texas Comptroller of Public Accounts under Government Code Section 2157.006(a)(2).²⁷⁵
- Emergency Procurement Exemption: State agencies are granted an exemption from the requirement to purchase IT commodities through a DIR contract if a situation arises in which compliance with Government Code Section 2157.068²⁷⁶ or 1 Texas Administrative Code Chapter 212²⁷⁷ is impractical or contrary to the public's interest, such as to prevent a hazard to life, health, safety, welfare, or property, or to

²⁷¹ 1 Tex. Admin. Code § 212.23(1); [One-Time Exemption Requests](#).

²⁷² [1 Tex. Admin. Code § 212.22](#). Pursuant to Texas Government Code § 2157.068(f), DIR created rules authorizing certain blanket exemption for discrete IT commodities that allow state agencies to procure the specific IT commodity exempted without needing to submit a one-time exemption to DIR. Blanket exemptions are reviewed regularly to ensure an ongoing need for the exemption.

²⁷³ As defined by 1 [Tex. Admin. Code § 212.1](#).

²⁷⁴ [Tex. Admin. Code § 212.1](#).

²⁷⁵ [Gov't Code § 2154.006\(a\)\(2\)](#).

²⁷⁶ [Gov't Code § 2154.068](#).

²⁷⁷ 1 Tex. Admin. Code Chapter 212.

avoid undue additional cost to the state. The scope and duration of the purchases shall not exceed the duration of the emergency.

- **WorkQuest Set-Aside Exemption:** State agencies are granted an exemption from the requirement to purchase IT commodities through a DIR contract if those items are offered in the WorkQuest catalog and designated by the Texas Workforce Commission as a product that is set aside from competitive bidding and offered through a DIR Cooperative Contract.

DIR also maintains [lists of ongoing and expiring blanket exemptions](#) on the DIR website.

Cooperative Contracts Exemption Request Processes

Generally, one-time exemption requests for Cooperative Contract purchases submitted to DIR must provide the following information:

- **Cost.** If a state agency determines the cost of procuring an IT commodity is less expensive through an avenue other than a DIR contract, the state agency must include in their exemption request to DIR the cost information, including the cost of making the procurement, the cost for implementation, any recurring costs over the term of the requested exemption, and any quotes received from a vendor.
- **Terms and Conditions.** If an agency determines that certain terms and conditions are not available through—and cannot be added to—the DIR contract, the state agency must include the terms and conditions, and the state agency requirement that is satisfied by those terms and conditions in the request.
- **Funding source restrictions.** If an agency encounters specific restrictions related to the funding source that would prevent it from procuring an IT commodity through a DIR contract, the state agency must include a description of those restrictions in the request.
- **Compatibility with existing technology infrastructure.** If an agency determines that its technological requirements cannot be delivered by an IT commodity available through DIR contracts, the state agency must include a detailed description of the compatibility issues in the request. The use of a particular hardware, software, or technology service by itself is not sufficient justification for exemption.
- **Proprietary restrictions.** If an agency encounters proprietary restrictions that would prevent it from procuring an IT commodity item through a DIR contract, it must describe those restrictions in the request.
- **Other circumstances or requirements.** If an agency has other extenuating circumstances or requirements that would justify why an IT commodity cannot be procured through a DIR contract, the state agency must include a description of the circumstances or requirements in the request.

State agencies requesting Cooperative Contracts exemptions must submit their request to DIR for review and approval. DIR has 15 business days from the date of receipt to evaluate and

either approve or deny the exemption.²⁷⁸

State agencies may request an expedited exemption.²⁷⁹ The expedited exemption request must include a statement from the head of the requesting state agency or their designee that describes the circumstances and justification for expedited review by DIR. DIR will process the expedited request and issue either an approval or denial within three business days of its receipt of the expedited exemption request.²⁸⁰

DIR will notify the requesting state agency of its decision to approve or deny the exemption request. The approval notification will include the specific scope, terms, requirements, and duration for which the exemption is approved. If the approval contains a scope, terms, requirements, or duration that is not as broad as the state agency's request, DIR will provide an explanation for the variance.

If the exemption request is denied, DIR will provide the state agency with a written explanation of the basis for the denial. A state agency that does not agree with the basis for denial may submit an appeal to the Legislative Budget Board.

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The IT Procurement and Contracting function is funded by fees collected through DIR's Cooperative Contracts, Shared Technology Services, and Communications Technology Services programs. The majority of funding comes from fees collected from the sale of technology commodities and services through the Cooperative Contracts program.

Figure 67 Method of Finance by Strategy

Strategy	Method of Finance	Amount
B.1.1 - Contract Admin.	Clearing Fund	\$3,618,946
B.2.1 - DCS	Statewide Technology Account	\$586,927
B.3.1 - Texas.gov	Statewide Network Applications Account	\$41,704
B.4.1 - Communications Technology Services	Telecommunications Revolving Account	\$492,613

²⁷⁸ [1 Tex. Admin. Code § 212.20.](#)

²⁷⁹ [1 Tex. Admin. Code § 212.21.](#)

²⁸⁰ [1 Tex. Admin. Code § 212.21\(a\).](#)

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

There are several other cooperative purchasing programs at the national, state, and local levels that offer some degree of technology products and services. Generally, these cooperatives select a government entity to lead the procurement. The lead entity then procures the products or services in a manner that meets its own state requirements and procurement rules. Each procuring entity must then negotiate their own additional customer-specific terms and conditions, including state-mandated provisions. In the case of cooperative programs such as the National Association of State Procurement Officials (NASPO), the lead government entity also generally charges an administrative fee above and beyond the fee already charged by the cooperative program. Those fees vary and may exceed the two percent maximum administrative fee statutorily approved for the DIR COOP program.

No other state has a technology cooperative program that rivals Texas' program. Utilization from public entities outside of the state is a testament to the uniqueness of Texas' robust program, in addition to its general success as well. Since 2019, more than 547 out-of-state governments have utilized DIR's COOP Contracts including 44 other U.S. states. Out-of-state utilization has grown by more than 129 percent since 2019. DIR solicits and negotiates contracts that meet state and local procurement rules, which allow for greater ease of use and competitive pricing (as baselined against other cooperative contract programs).

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

DIR's HUB Program collaborates with various minority- and women-owned business trade organizations and development centers to circulate information pertaining to the initiatives of the Statewide HUB Program through the Texas Comptroller of Public Accounts.

HUB certification provides vendors an opportunity to do business with DIR's eligible customers to increase HUB spending. DIR has adopted the Statewide HUB Program rules as its own. Both DIR and the Comptroller of Public Accounts follow certain processes to ensure the best value to the state for IT/automated information system commodities and services, which can be provided to the State of Texas.

The DIR HUB Program coordinates efforts for education and training across the state. DIR created the HUB Talk Series and coordinated virtual trainings to further educate the vendor and customer community on all procurement related activities across the state. DIR co-sponsors and supports Comptroller of Public Accounts-related events (such as spot bid fairs). DIR and the Comptroller of Public Accounts meet throughout the year to discuss partnering opportunities.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

Eligible local, regional, or federal units of government of the DIR Cooperative Contracts Program include:

- Local governments, including counties, municipalities, school districts, and junior college districts;²⁸¹
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.²⁸²

DIR's IT Procurement and Contracting function interacts with other units of government in various ways as described below.

Texas Comptroller of Public Accounts

The Texas Comptroller of Public Accounts' Statewide Procurement Division (SPD) is the central authority for state agency procurement guidance, education, and statewide contract development services. SPD publishes the State of Texas Procurement and Contract Management Guide to aid public procurement professionals in the execution of their duties by providing step-by-step guidance and a framework for the continued development of public procurement processes and best practices. DIR's IT Procurement and Contracting function activities are developed in alignment with the framework described in the Texas Procurement and Contract Management Guide. DIR also works closely with SPD as necessary, and particularly following legislative cycles, to develop specific IT procurement practices for inclusion in the Procurement and Contract Management Guide.

DIR also coordinates with the Comptroller of Public Accounts to provide training for the Certified Texas Contract Developer (CTCD) and Certified Texas Contract Manager (CTCM). These trainings include information on DIR's background, statutes for procurement methods, STS, COOP, IT thresholds, explanations for the statement of work and exemption process, determining IT procurement methods, and HUB Program.

Managed Customer Contracts

As described in the Chief Procurement Office Process Guide, DIR establishes managed

²⁸¹ [Gov't Code § 2054.003\(9\)](#).

²⁸² [Gov't Code § 2157.068\(j\)](#); *see also* [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\)](#).

customer contracts to structure procurement and contracting activities with eligible customers as provided in statute, or other government entities from whom DIR wishes to obtain products or services. These contracts include:

- **Interagency Contract** – eligible state agency customers must execute an interagency contract to access programs within STS.
- **Interlocal Contract** – customers other than state agencies must execute an interlocal contract to access programs within STS.
- **Texas Statewide Data Exchange Compact** – a memorandum of understanding through which DIR and state agencies coordinate the sharing of interagency data.
- **Interstate Cooperative Contract** – eligible out-of-state customers must execute an interstate cooperative contract to access DIR's Cooperative Contracts.

k) If contracted expenditures are made through this program please provide:

A Short Summary of The General Purpose of Those Contracts Overall

The IT Procurement and Contracting program is responsible for providing procurement and contract management services for the entire agency. The program utilized contracts during fiscal year (FY) 2022 primarily for staff augmentation to support the growing number of services that the agency delivered during 2022.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$893 thousand in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 37 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from March 2021 through August 2022 for these contracts. The funding sources for these contracts include revenues from the Cooperative Contracts and communications and technology services programs.

The Method Used to Procure Those Contracts

The methods used to procure these contracts were request for quote, TXSmartbuy, open market, request for qualifications, and direct award.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-CPO-4642	WorkQuest	Provide staff augmentation services for DIR.	\$276,882.29
DIR-CPO-4634	Sourceplus LLC	Provide staff augmentation services for DIR.	\$265,775.60
DIR-CPO-4529	Internal Data Resources Inc.	Provide staff augmentation services for DIR.	\$143,866.60
DIR-TSO-4099/RFQ-12-FY21-SA0002	Gartner Group	Provide research and advisory services for ELT.	\$82,185.77
DIR-CPO-4617/RQ17-FY22-SA-0022	Indotronix International Corporation	Provide staff augmentation services for DIR.	\$21,153.30

The Methods Used to Ensure Accountability for Funding and Performance

DIR's contract and vendor management processes ensure that contractors perform in accordance with all contractual requirements. Active management of service level agreements also ensures that vendors deliver in accordance with each contract.

A Short Description of Any Current Contracting Problems.

Not applicable.

l) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

DIR's IT Procurement and Contracting function is impeded by challenges related to agile procurement, harmonization among procurement statutes, and the lack of an IT procurement stakeholder workgroup.

Agile Procurement

Often, traditional government procurement models do not keep pace with the evolution of technology. The traditional process begins with agency planning during the Legislative Appropriations Request process before obtaining approval during a legislative session. The open procurement process may take a year or potentially even longer (depending on the size and scope of the procurement).

Due to the speed at which it changes, technology and an agency's requirements may have

changed before these processes can be completed. The agile procurement method focuses on shorter timeframes for quick, informed decision-making and faster contract awards. Because agile procurement facilitates flexibility and adaptability, the federal government has moved towards this methodology, which has resulted in faster delivery of IT products.²⁸³ Though Texas procurement statutes ensure transparency and accountability, they do not readily adapt to agile procurement methodologies. One way to improve IT procurement would be to revise existing procurement statutes to allow agile procurement methodology while still requiring transparency and accountability in this process.

Procurement Statute Harmonization

Because Texas procurement statutes contain both broad, general procurement requirements and niche, targeted mandates for IT procurements, compliance obligations can be ambiguous and difficult to determine. For example, [Government Code Chapter 2157](#) establishes IT procurement requirements specifically for Cooperative Contracts; however, broader procurement rules exist in other chapters of the code that either do not reference [Government Code Chapter 2157](#) or directly conflict with its requirements. Thus, confusion exists about the applicability of certain statutory requirements to technology procurements. Revising these statutes to clarify the application of general procurement requirements to IT procurements could improve the efficiency of IT contracting in addition to increasing transparency, accountability, and DIR's ability to obtain the best value for the state.

IT Procurement Stakeholder Workgroup

The legislative creation of a stakeholder workgroup that consists of representatives from state agencies, legislative staff, and the vendor community could be especially helpful to the statutory revision efforts. The workgroup could analyze both general procurement statutes and the technology procurement statutes and identify recommended changes that could reduce or eliminate confusion and facilitate agile methodology in Texas IT procurement and contracting.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

The COOP program generates hundreds of millions of dollars in cost avoidance each fiscal year. By leveraging the purchasing power of the state, DIR negotiates technology contracts and provides efficient and cost-effective delivery of products and services.

DIR competitively procures these contracts in compliance with state law, negotiates base terms and conditions, and offers substantially discounted prices for IT products and services. DIR's initial work allows eligible customers to quickly and easily procure necessary technology goods

²⁸³ "Agile Government: Building Greater Flexibility and Adaptability in the Public Sector." Deloitte, March 2021: <https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-trends/2021/agile-at-scale-in-government.html>

and services to fulfill their missions.

o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility). For each regulatory program, if applicable, describe:

Although DIR is not a regulatory agency, DIR is tasked with the following requirements related to the IT Procurement and Contracting function.

Statement of Work Reviews

Why the Regulation Is Needed

State agencies are required to submit certain statements of work to DIR for review and approval before they solicit vendors for projects with an award value of more than \$50,000. DIR must review and sign the final statement of work before the state agency can pay any money to a selected vendor. State agencies must follow threshold requirements for IT commodity items. DIR's review of the statement of work is to ensure an agency's compliance with the black-and-white statutory requirements for these types of projects.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

State agencies submit their draft and final statements of work to DIR for review and approval through the DIR SOW Portal. DIR has 30 days from a state agency's submission of its statement of work to review and make recommendations based upon its statement of work checklist, which acts as a guide to ensure that legislative requirements are included in the statement of work. If DIR notes any concerns, DIR communicates those concerns to the agency. The agency is then provided with the opportunity to revise the statement of work to address the concerns.

Follow-up Activities Conducted When Non-compliance Is Identified

When DIR identifies that a state agency is non-compliant with the statement of work requirements, DIR contacts the agency by email. If an agency did not submit a statement of work to DIR for review and approval before completing a procurement,²⁸⁴ DIR must review and sign the final statement of work before the state agency can disburse funds to a vendor since the statement of work is not valid and any invoices cannot be paid. While DIR does not have the authority to audit agencies to ensure compliance with statement of work requirements, the State Auditor's Office conducts agency audits, which may identify these issues dependent upon the audit's scope.

Actions Available to the Agency to Ensure Compliance

DIR does not monitor agency procurements and relies on agency submission of statements of work for compliance. DIR is not required to report an agency's non-compliance with these

²⁸⁴ [Gov't Code § 2157.0685](#).

requirements, nor do we report non-compliance to any entity. DIR also does not include non-compliance as a peripheral inclusion in any report.

In addition, DIR is not required or authorized to conduct agency audits with respect to statements of work.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Exemptions Processing

Why the Regulation Is Needed

Per [Government Code Section 2157.068](#), state agencies are required to submit exemptions for DIR to review and approve prior to soliciting vendors for a contract with an award value which will exceed \$10,000.²⁸⁵ DIR must review and approve exemptions prior to purchase.

DIR reviews exemptions to assist agencies in complying with legislative mandates to utilize DIR contracts for IT commodity purchases. DIR's exemption process offers agencies the ability to procure IT commodities that may not be available—or otherwise satisfied by an offering available—through a DIR contract.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

State agencies submit their exemptions to DIR for review and approval through the DIR Exemption Portal on the DIR website. DIR has 15 days from submittal of an exemption to review and approve or deny the exemption using an exemption form to ensure that exemption requirements are met. If DIR notes any concerns during its review, DIR communicates those concerns to the agency and provides them the opportunity to revise the exemption and address any concerns.

Follow-up Activities Conducted When Non-compliance Is Identified

When DIR identifies that a state agency is non-compliant with these requirements, DIR contacts the agency by email. If an agency does not submit an exemption to DIR for review and approval before completing its procurement, DIR does not have the authority to audit the state agency to determine compliance. The State Auditor's Office may determine that the state agency was non-compliant with this requirement, dependent upon the audit's scope.

Actions Available to the Agency to Ensure Compliance

DIR does not monitor agency procurements and relies on agency submissions of exemptions to determine compliance. DIR is not required to report an agency's non-compliance with these requirements, nor do we report non-compliance to any entity. DIR also does not include state

²⁸⁵ [Gov't Code § 2157.068](#).

agency non-compliance with this requirement as a peripheral inclusion in any report.

In addition, DIR is not required or authorized to conduct agency audits with respect to exemptions.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Shared Technology Services



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.

a) Provide the following information at the beginning of each program description.

Name of Program or Function: Shared Technology Services

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Dale Richardson, Chief Operating Officer

Statutory Citation for Program:

[Government Code Chapter 2054, Subchapter L, Statewide Technology Centers](#)

[Government Code Chapter 2054, Subchapter O, Major Outsourced Contracts](#)

[Government Code Chapter 2059, Texas Computer Network Security System](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.

Exceptional
Total Experience



Compliance
First



Value Through
Technology



Secure
Texas



Operational
Excellence



The objective of DIR's Shared Technology Services (STS) function is to supply a set of managed information technology services that are secure, modern, mature, and reliable so that, rather than directly managing IT services, Texas government organizations can focus on serving Texans and supporting business functions.

STS includes public and private cloud solutions, mainframe, application development and

maintenance, managed security services, and digital commerce. To minimize risk and ensure the highest quality, each service is provided by best-in-class vendors, incorporating leading industry standards and proven best practices in an innovative, flexible, and agile manner.

STS harnesses the collective size and volume of Texas government to make enterprise class, best-in-industry technology services (once only feasible for very large organizations) attainable for even the smallest state agency. When agencies handle their own IT operations, they get the best that their IT team can offer and the best that their funding can support. Through STS, state agencies receive the best the entire industry – and Texas – has to offer.

STS includes two statewide technology centers (Data Center Services, or DCS, and Application Services Center), Texas.gov, Managed Security Services, and the Open Data Portal, which are all managed by the Multi-sourcing Services Integrator (MSI).

As authorized by [Government Code Section 2054.378](#), DIR may directly operate or contract with another entity to operate statewide technology centers to provide government entities, on a cost-sharing basis, services related to information resources and information resources technology and the deployment, development, and maintenance of software applications.²⁸⁶

DIR branded the first statewide technology center “Data Center Services (DCS)” because the Texas Legislature’s requirements initially included server, mainframe, and bulk print and mail services. Subsequently, DIR established the Application Services Center to address DCS customers’ legacy modernization and cybersecurity challenges with application development and maintenance. This change is consistent with the modern state of the software application marketplace. Application software generally means software intended to perform discrete functions for an end user that are unrelated to the operation of the computer itself, and today is often bundled together with the use of hardware and software necessary for the application to function. Access to the whole package is then delivered based on a periodic subscription for a recurring fee. Because these hardware and non-application software services would have traditionally been provided through the Data Center Services program, DIR integrated these additional services with the DCS program to provide customers a seamless service delivery approach. Application services are available for customers whose applications are hosted in either the DCS public or private cloud.

The model below identifies services by each statewide technology center.

²⁸⁶ [Gov’t Code § 2054.378](#).

Figure 68 Data Center Services

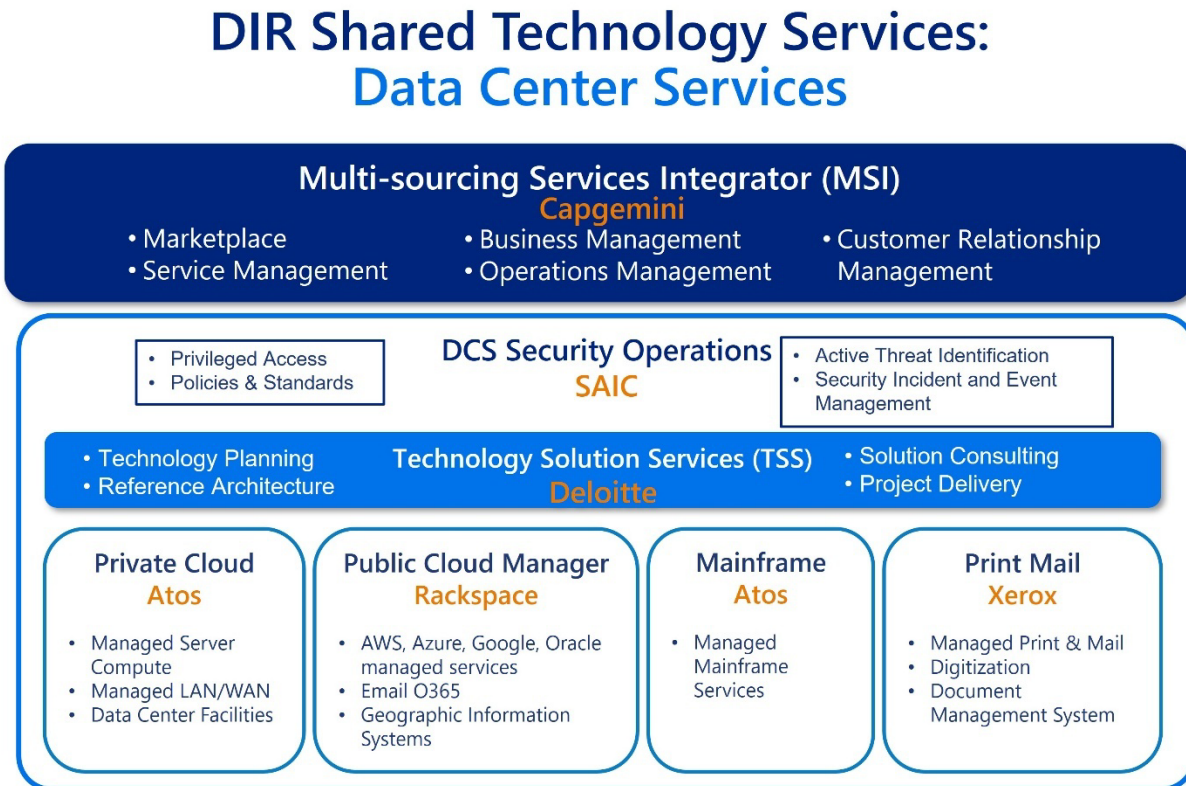
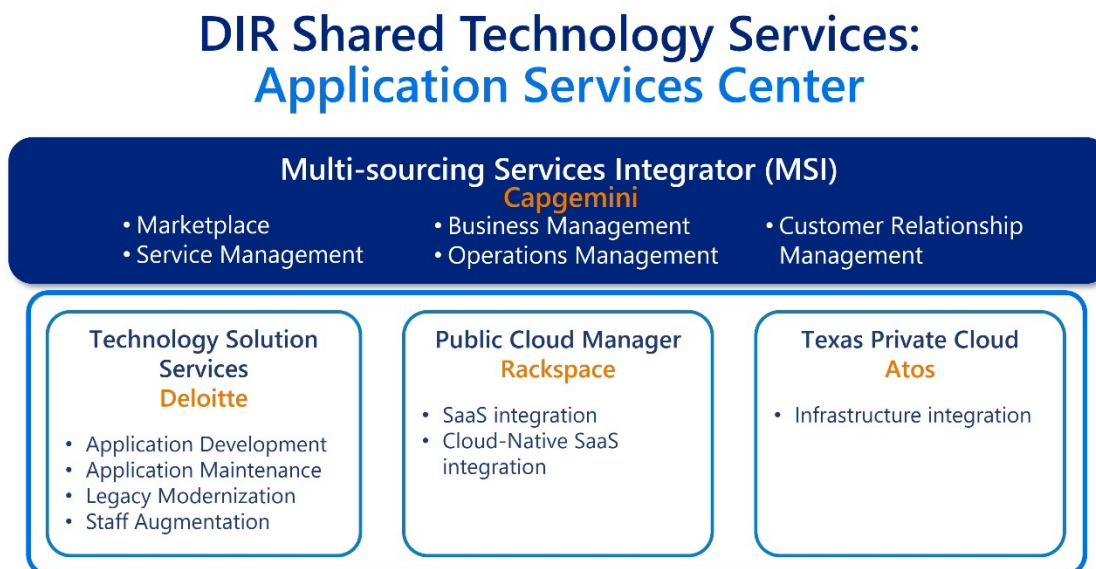
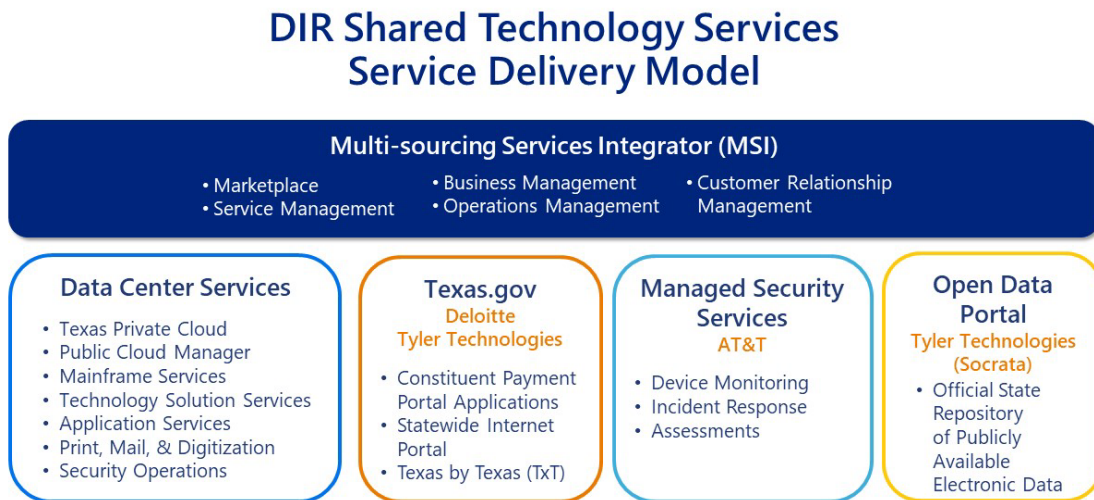


Figure 69 Application Services Center



The model for how DIR delivers these services is depicted below.

Figure 70 Service Delivery Model



The **Multi-sourcing Services Integrator (MSI)** gives DIR’s customers a single point of entry into all STS programs. DIR contracts with Capgemini to manage and integrate STS for customers, standardize processes, administer enterprise service components, and maintain the STS Customer Portal.

The **Data Center Services (DCS)** program provides IT services delivered through outsourced contracts, including:

- Texas Private Cloud, which provides server compute, pre-configured security solutions, data center facilities, and network management services for DIR’s government customers from the state’s two Consolidated Data Centers. Through the Texas Private Cloud, customers receive resilient compute with automatic failover, the ability to resize their compute on demand, and the ability to decommission and stop paying for services they no longer need. DIR contracts with Atos Governmental IT Outsourcing Services, LLC (Atos), to manage two Criminal Justice Information Security compliant, redundant, and resilient Consolidated Data Centers, one in Austin and one in San Angelo.
- Public Cloud Manager, which provides public cloud services through public cloud infrastructure and platforms across four public cloud service providers (Amazon Web Services or AWS, Azure, Google, and Oracle) that implement best practices and provide technical and security assurances. DIR contracts with Rackspace US, Inc. (Rackspace) to integrate, provision, and manage the public cloud service providers.
- Mainframe Services, which provides mainframe-based computing, technical solutions, data center facilities, and network management services for DIR’s government customers from the Consolidated Data Centers. DIR contracts with Atos to manage mainframe services delivered in a shared consumption model, structured to allow customers to migrate off mainframe technology without stranded assets or costs.

- Technology Solution Services (TSS) provides infrastructure strategy management, solution design, and project delivery in the DCS public and private clouds. DIR contracts with Deloitte Consulting, LLP (Deloitte) to deliver technical strategy management, solution design, and project delivery and supply managed application services for applications hosted in DCS public and private infrastructure.
- Print, Mail, and Digitization, which provides print impressions, mail insertion per envelope (which includes all folding, letters, inserts, and business reply envelopes), and digital delivery of documents using a system that tracks all documents from receipt through completion. DIR contracts with Xerox Corporation (Xerox) to provide high-volume printed documents mailed to constituents, taking advantage of volume postage savings, and digitization services to reduce printed documents.
- STS Security Operations delivers enterprise security services by establishing program standards and providing an enterprise security incident and event monitoring solution, privileged access management, digital forensics, and advanced threat hunting. DIR contracts with Science Applications International Corporation (SAIC) to provide cybersecurity policies, monitoring, and independent security oversight of DCS infrastructure.

The **Application Services Center** provides the development, deployment, and maintenance of software applications, including the procurement, configuration, and integration of Software-as-a-Service (SaaS) and cloud computing services as defined by rule.²⁸⁷ The Application Services Center:

- Addresses the technology industry's evolution of software and infrastructure services into a combined SaaS technology and includes both infrastructure (DCS) and application software (Application Services).
- Ensures that cloud-based applications connecting to—or interfacing with—the DCS environment are safe, secure, and properly managed for the good of the state's shared technology infrastructure. This interfacing includes leveraging the DCS program vendors to vet, procure, and integrate such products when they are adopted by DCS customers.
- Includes TSS, which provides application development services including development, maintenance, and staff augmentation services for applications hosted in the DCS public and private clouds.
- DIR contracts with Deloitte to provide:
 - Legacy modernization services;
 - Application development and maintenance; and
 - Application staff augmentation resources.

²⁸⁷ 1 Tex. Admin. Code §§ [215.43](#), [215.53](#).

Managed Security Services (MSS) program provides a select set of security services in three functional categories containing multiple offerings to meet the modern security needs of Texas government and allow eligible entities to leverage DIR's pre-negotiated, highly competitive pricing to receive these offerings. DIR contracts with AT&T Corp. (AT&T) to provide:

- Security monitoring and device management.
- Security incident response.
- Compliance and risk management.

Please note that information on the **Texas.gov** and **Open Data Portal** programs, though administered by STS, are considered separate functions, and are included in distinct Key Functions of this Self-Evaluation Report. **MSS** is also discussed in VII. Guide to Agency Programs - Cybersecurity.

c) What information can you provide that shows the effectiveness and efficiency of this program or function?

STS provides services to designated entities required to participate in the DCS program²⁸⁸ and discretionary customers who voluntarily join the program for one or more services. In 2017, DIR integrated the Texas.gov program into STS. Additionally, Texas.gov infrastructure is hosted and managed by DCS. STS also offers optional application services to DCS customers and optional security services to all DIR customers.

DIR monitors the effectiveness and efficiency of the Shared Technology Services function through customer growth and use of the STS programs in addition to vendor performance and customer satisfaction ratings. The data in this section includes all STS programs.

Customer Growth and Usage

STS metrics demonstrate customer satisfaction, effective vendor performance, and efficiencies for the state. Statistics from FY22 show:

- STS serves 557 state and local government entities.
- 73 new customers were added in the last fiscal year, representing a 16 percent growth from FY21.
- MSS is the most utilized STS with 96 percent of STS customers utilizing an available service offering.
- 59 customers leverage three or more programs made available through STS.

²⁸⁸ [Gov't Code Chapter 2054, Subchapter L.](#)

Figure 71 STS Metrics

Designated Customers	Program	Discretionary Customers
25	DCS	90
25	MSS	512
21	Texas.gov	58
22	ODP	20

Data Center Services (DCS) infrastructure growth and migration to public cloud capabilities:

- 24 percent of customers are in four public clouds managed with DCS security assurances.
- 76 percent of customers are in the private cloud, leveraging the data center facilities at Angelo State University.

Digital Transformation through Print, Mail, and Digitization:

- Printed 351 million pages and mailed 85 million envelopes.
- Delivered 35 million digital documents, which saved 339 trees and removed the equivalent emissions of 21 cars.

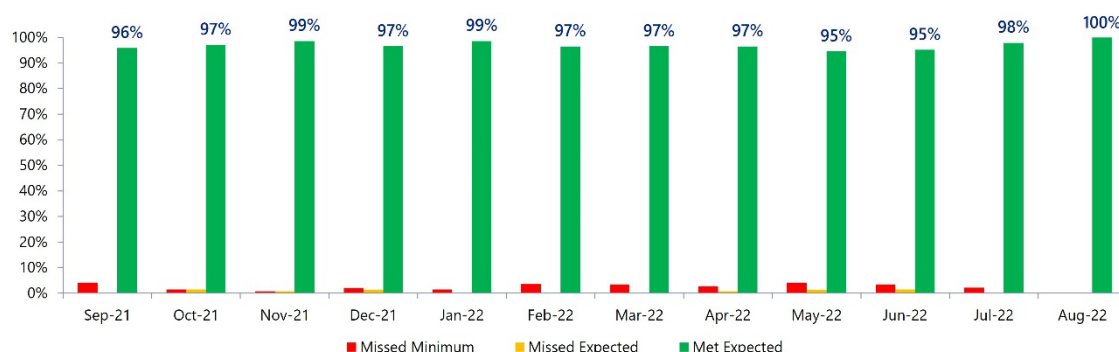
Vendor Performance Ratings and Customer Satisfaction Scores

Vendor Service Level Agreements

DIR tracks compliance with service metrics agreed upon between DIR and service providers across the STS programs. Service level agreement performances are published to STS customer dashboards each month. In FY22, an average of 97 percent of vendors met all service levels.

Figure 72 Service Level Agreements

Shared Technology Services – Performance Management Service Level Agreements (SLAs)



Monthly Customer Scorecards

STS customers enter monthly detailed scores on the STS vendor performances, and on average, 95 percent report satisfaction with STS services.

DIR evaluates these scores and addresses any vendor shortcomings. DIR then reports the scorecard results quarterly to DIR’s Board of Directors and Board subcommittees.

The chart below reflects the overall customer satisfaction rating for FY22 with 100 percent satisfaction achieved in March and August 2022.

Figure 73 Customer Satisfaction Monthly Scorecard

Shared Technology Services – Customer Satisfaction

Monthly Scorecard



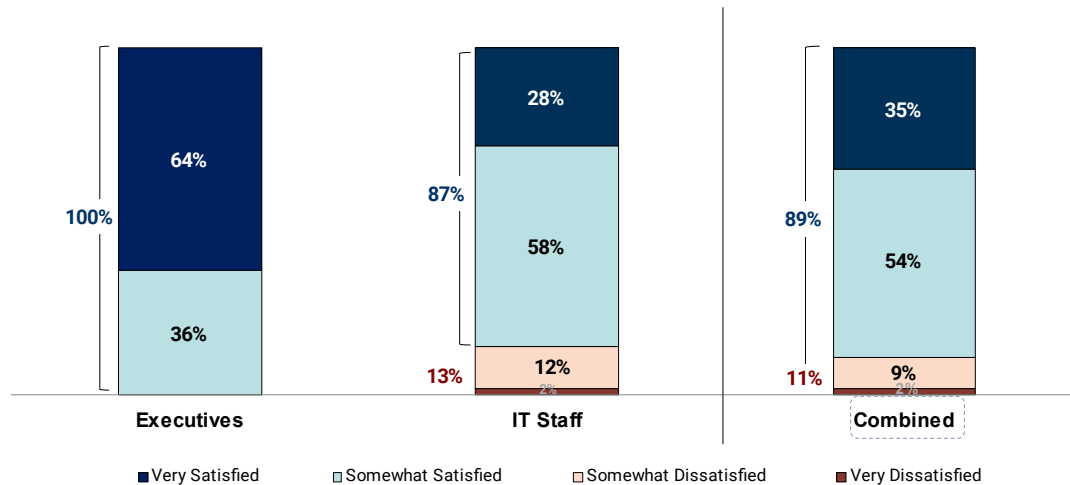
Independent Third-Party Customer Satisfaction Survey

DIR engages an independent third-party vendor to survey all STS customers annually. The MSI uses the results of that survey to drive program improvements alongside the STS vendors. Survey results are shared with—and analyzed by—the STS Owner-Operator Governance structure to identify customer-related improvements and needs. Customer satisfaction is measured in two groups: business executives and IT staff. Results are both compared and combined to identify needs and trends. Results from the customer satisfaction survey that was conducted in January 2023 show:

Figure 74 Overall STS Satisfaction

Overall STS Program Satisfaction Executives vs. IT Staff vs. Combined

Please rate your OVERALL satisfaction with the services provided to your organization through the STS program.

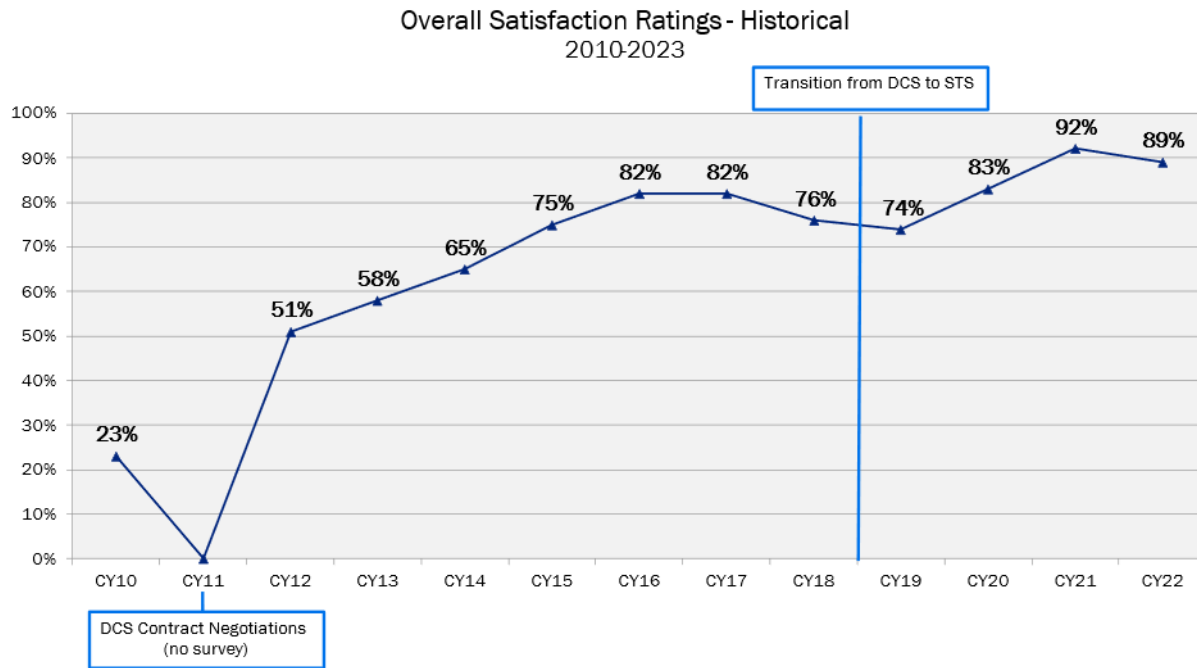


2

Historically, the third-party customer satisfaction survey results have consistently shown high levels of satisfaction as presented in the graph below by calendar year (CY). Note: CY11 was a re-procurement year with no surveys.

The performance measure is defined as “% of Customers Satisfied with Data Center Services Contract Management” and is reflected in the annual survey as “Overall Job Performance Rating of DIR.” Originally, DIR reported the performance measure based on responses from agency business executives only. This small group of customers is not traditionally involved in DIR’s day-to-day interactions and has little to no knowledge of how DIR performs contract management. DIR has found it challenging to receive timely and informed survey responses from business executives. A more accurate measure of DIR’s performance would gauge customer satisfaction with DIR’s services, customer satisfaction with STS overall, or a survey aligned with the STS’ monthly scorecard questions. Additionally, these responses only measure a “single point in time.” Assessing those responses over the course of a full year would be better than reflecting how a customer agency feels about DIR at one particular moment in the year. Considering the preceding challenges with this performance measure, the LBB changed it in the 88th Legislative Session seeking more consistent and accurate data by referencing DIR’s monthly customer surveys as a measure of performance.

Figure 75 Overall Satisfaction Ratings-Historical



The STS Value

STS strives to provide excellent value for taxpayer dollars in terms of the variety of robust services, security protocols, and industry-leading providers supplied. Technology solutions that were once feasible only for large organizations with significant budgets are now available to DIR customers of all sizes and budgets.

Because legacy systems create and increase risk for the state, STS assists participating DCS customers with updating software and upgrading hardware to reduce the security and reliability concerns associated with legacy systems.

STS was designed and built for the high-security needs of government. Agencies must have security surrounding their data and business. STS provides an additional level of protection and prevention with the industry's best monitoring and operational maintenance. STS provides the complete security package: protecting, preventing, watching for, and catching criminals from getting unintended access to Texas' data and systems.

Texans' growing demand for online government services is driving digital transformation at the state level. STS facilitates an organization's digital transformation with modern technology—and at accessible prices.

STS provides entities with technical expertise and responsive support that frees up critical IT workforce resources for an organization to focus on its mission. At a time where state IT workforce turnover is tumultuous, outsourcing management of IT resources to STS ensures continuity and reliability for mission-critical tasks.

STS Value for Small Agencies

What would it cost for a small agency to build an IT department that met the same level of security, reliability, and disaster recovery as STS? Using a small agency that migrated their infrastructure to STS, DIR compared the STS cost estimate to an estimated cost for that agency to deliver equivalent technology standards on their own.

The example agency had several critical applications on approximately a dozen servers.

If this agency were to develop a secure, reliable, recoverable infrastructure to the level of the Data Center Services program, the agency would need to invest about \$750,000 to develop and roughly \$2.4 million per year to maintain. In contrast, this agency can migrate their IT to STS for approximately \$155,000 one-time costs and between \$220,000 to \$290,000 annual maintenance. The primary driver of this vast difference in cost relates to DIR's ability to provide enterprise class technology and security so that DIR's customers share in the cost rather than bear the whole cost.

Security in STS Programs

STS provides robust security tools and protocols for keeping state information systems safe. With an added layer of security interwoven throughout the function, customers have the peace of mind that comes with knowing they have continuous protection with state-of-the-art security solutions.

STS was designed and built to address the high-security needs of government even as cyber threat actors grow increasingly sophisticated and capable of adapting to the changing technological landscape.

Every state agency must have security protocols in place to protect their data and business; however, good security does not stop there. Agencies must also ensure that they have rigorous monitoring and operational maintenance of their networks and infrastructure. STS provides that additional level of protection and prevention in support of DIR's mission to analyze cybersecurity risks to the state and empower state and local governments with reliable and secure technologies.

In conjunction with the offerings made available through DIR's Cybersecurity function, STS allows DIR to provide a complete security package to state agencies.

Security in the Cloud

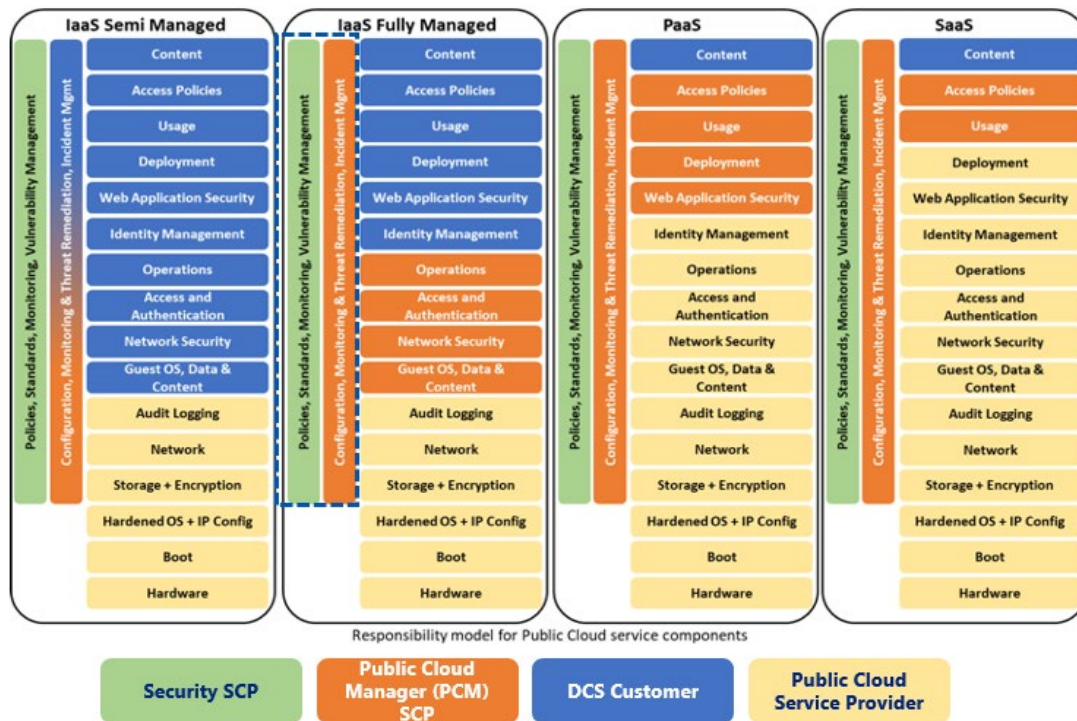
The complexities of cloud computing provide challenges when trying to secure various cloud environments. Users of cloud services are responsible for the security of their data in the cloud, but STS provides another layer of security and mitigates risk by providing:

- Defined security policies, standards, and baseline configurations;

- Solution blueprints with embedded security configurations and ongoing configuration inspection;
- Detection and response to negligent or malicious threats, including malware protection and penetration identification;
- Visibility of user activity, privileged user threats, and compromised accounts;
- Security incident remediation; and
- Cybersecurity assessments.

Through STS, users can optimize security in the cloud more efficiently and cost-effectively than if they were to implement cloud services on their own. As the image below shows, the more cloud management an agency defers to STS service component providers, the more security controls are implemented and monitored by the program.

Figure 76 Responsibilities for Security in the Texas Public Cloud



d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

2005

The 79th Legislature passed [House Bill 1516](#), which directed DIR to consolidate and standardize state agencies' IT infrastructure, products, and services with large investments in IT to reduce statewide costs, modernize aging state infrastructure, increase overall security, and improve

disaster recovery capability.²⁸⁹ The passage of this bill signaled a larger adoption of a statewide shared IT infrastructure, first conceptualized back in 1993 with the incorporation of the General Appropriations Act (GAA) rider outlining DIR and Angelo State University's collaboration on the creation of the State Data Recovery Facility and Operational Data Center at Angelo State University. Additionally, lawmakers sought to stay current with IT best practices and reduce risks associated with disaster recovery, security, and critical state data and system assets backup.

2006

DIR selected 29 state agencies to participate in the data center consolidation and collaborated extensively with these agencies to develop the DCS request for offer and conduct the procurement for outsourcing the management of these agencies' IT infrastructure.

2007

DIR entered into a contract with International Business Machines (IBM) for the provision of server, mainframe, and bulk print and mail services, and to consolidate the infrastructure and associated managed services. As part of this effort DIR consolidated more than 31 disparate, legacy data centers into two highly secure, redundant data centers in Austin and San Angelo.

2010-2011

DIR restructured DCS into a service integration model with multiple service component providers and a Multi-sourcing Services Integrator (MSI) that positioned the state to better achieve more flexibility, accountability, and functionality, and better involve customer agencies in the decision-making process. DIR began the re-procurement of DCS services with DIR's release of two Data Center Services requests for offer.

2012

DIR awarded three contracts for DCS-related services:

- Multi-sourcing Services Integrator (MSI) to Capgemini;
- Server and Mainframe Services to ACS Technologies; and
- Bulk print and mail to Xerox.

2016

DIR met the consolidation goal of the enacting legislation, with mainframe, print and mail, server, and service desk services fully consolidated. Consolidation of server technologies was much more complex and difficult for STS customers, and 100 percent physical consolidation was not technically feasible. Therefore, DIR established a goal for customers to consolidate 75

²⁸⁹ [Acts 2005, 79th Leg., R.S., ch. 1068 \(H.B. 1516\), 2005 Tex. Gen. Laws 3544, 3546 \(codified at Gov't Code Chapter 2054, Subchapter L\).](#)

percent of their server compute. By the end of 2016, DIR had achieved that goal.

2017

DIR continued to expand the offerings available to eligible customers through the STS when it awarded two managed application services contracts. These contracts added managed application services for application development and maintenance, and application services staff augmentation. Furthermore, these contracts allowed customers to reinvest infrastructure consolidation savings to continue modernizing legacy applications. In addition to these managed application services contract additions, DIR also began expanding its STS offerings to include hybrid public cloud capabilities.

2018

DIR awarded two contracts under the Texas.gov procurement. Under these contracts, two separate vendors would provide the services necessary to support Texas.gov: Deloitte provided the Texas.gov application development services and Texas NIC (now called Tyler Technologies) provided the Texas.gov payment processing. Due to the growth and critical nature of the Texas.gov program, DIR added it to DIR's outsourced managed services provided through the DCS program. Additionally, DIR executed a digital Multi-Sourcing Services Integrator (MSI) that further enhanced the abilities of the program. Together, these contracts expanded the DCS program with DIR rebranding it as the STS to reflect this expansion.

Also in 2018, within the newly rebranded STS, DIR established the Managed Security Services (MSS), which provided various security services to customers eligible for STS. Through the MSS program, DIR was able to provide penetration tests and Texas Cybersecurity Framework (TCF) assessments for state agencies and institutions of higher education; the MSS further ensures the security of the state's data and networks by making available to eligible customers other types of assessments, penetration tests, incident response services, security monitoring services, and device management services. The Cybersecurity Operations team also utilizes security operations center services through MSS.

2019

DIR launched the Texas by Texas (TxT) program, with the Texas Department of Licensing and Regulation as the first state agency to use it to process massage therapist license renewals. Additionally, DIR began its solicitation of the Next Generation Data Center Services for:

- Texas private cloud, facilities, and computing services;
 - Technology solution services;
 - Print, mail, and digitization services;
 - Security operations services;
 - Public cloud manager; and
 - Mainframe services.
-

2020

In 2020, DIR introduced TSS and SecOps, further enhancing the STS technical solutioning and

security operations capabilities. Previously, under the original Managed Application Services contract, customer agency use of application development and maintenance was minimal. When these same services were procured in 2020 as part of the next-gen DCS contract, DIR ensured the new TSS concept more closely aligned with our customer agency business objectives to better serve customer business needs and their strategic objectives. The new model has increased the value to STS agencies and their constituents with great success and customer satisfaction. Beyond just planning technology solutions, TSS develops, modernizes, and maintains applications within STS. These services are available as managed services or via staff augmentation, benefiting DIR customers and vendor partners alike. In the next iteration of TSS, DIR plans on researching using multiple vendors to support agency application projects and limit total project costs to less than \$10M.

DIR also separated public and private cloud management into two separate contracts to attract best-in-breed technology providers.

DIR awarded multiple contracts supporting the Next Generation DCS model, including:

- Texas private cloud, facilities, and computing services;
- Technology solution services;
- Print, mail, and digitization services;
- Security operations services;
- Public cloud manager; and
- Mainframe services.

2021

DIR amended the [1 Texas Administrative Code 215](#) provisions governing statewide technology centers to address significant changes in recent years to the way technology products are delivered and utilized; these changes also addressed the shift toward cloud-based offerings and more highly specialized or configurable applications, and the state's acceleration of its use of these new offerings as a result of the COVID-19 pandemic.²⁹⁰ The amendments to these rules became effective August 2021 and included the creation of a new statewide technology center—the Application Services Center—after DIR obtained the approvals required by law.²⁹¹

The creation of this new center was necessary because the technology industry has quickly evolved software and infrastructure services into a combined Software-as-a-Service (SaaS) model. Furthermore, the technology industry has introduced other trends that blur the lines between software applications and traditional data center services. Because SaaS includes both infrastructure (DCS) and application software (Application Services), the two statewide technology centers are legally separate but interact seamlessly in practice; however, DIR anticipates that increased adoption of cloud-driven technologies will transition more and more

²⁹⁰ [1 Tex. Admin. Code ch. 215](#).

²⁹¹ 1 Tex. Admin. Code Chapter 215, Subchapters [D](#) and [E](#).

products and services traditionally associated with DCS to the Application Services Center. By creating this new center, DIR seeks to effectuate the Legislature's intent for the DCS, while keeping pace with changes in the technology marketplace.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The following entities are eligible for services DIR provides, including programs within the Shared Technology Services function:²⁹²

- State agencies;
- Local governments;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state, or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Tax Code Section 152.001; and
- Government entities of another state.

²⁹² Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

Figure 77 Breakdown of Entities Affected

Entity Type	Count
K-12 Schools	51
Local - City	32
Local - County	254
Local – Mental Health	1
Local – Other (Library District)	1
Other – Assistance Org	3
Other – Hospital District	3
Other – Local Govt Corp	1
Other – Utility District	4
Other – Water Authority	9
Political Subdivision	27
State – Agency	96
State – Higher Ed	42
State – Public Jr Colleges	33
Total	557

f) Describe how your program or function is administered, including a description of the processes involved in the program or function.

STS Administration

The Shared Technology Services function, including all the programs within STS, is administered by the Chief Operations Office (COO) with input from—and collaboration across—all DIR divisions. DIR's Chief Operations Officer oversees all of COO, which includes the Vendor Management Office, STS Project Engineering team, STS Operations team, STS Customer Service team, STS Financial Analysis team, STS Contract Management team, and Multi-sourcing Services Integrator (MSI).

The Vendor Management Office is responsible for managing the relationship between DIR and STS vendors by managing communications to and from the vendor; monitoring performance metrics and service and operations oversight; and identifying risks by assessing vendors, risk monitoring, and risk mitigation. Eight Vendor Managers manage the STS service providers. The Governance Program Manager manages the STS owner-operator governance model. The Technology Director oversees and directs STS vendors' technology strategy, reference architecture, and roadmap. This team reports to the Director of STS Vendor Management.

The STS Project Engineering team is responsible for providing enterprise oversight and management of STS portfolios, programs, and projects. In addition, the team ensures the implementation of enterprise, critical, customer, refresh, and service evolution projects; consistent, compliant service delivery execution by DIR and STS vendors; the service

management manuals for the STS; the STS process improvements with the STS service providers; and standard operating procedures for the Chief Operations Office (COO). This team is led by the Director of STS Project Engineering, who oversees four System Analysts and two Portfolio Project Managers.

The STS Operations team is responsible for managing the STS vendors' delivery of services. The team monitors vendor service delivery to customers; identifies and resolves issues; ensures availability, security, and recoverability of customer data and infrastructure; provides network security operations; and oversees enterprise infrastructure change management. The STS Operations team includes five STS Operations System Analysts and the Assistant Director of STS Operations, who all report to the Director of Program Operations. The team provides expert information and advice regarding server, network, mainframe, and data center environments in addition to overall guidance to the STS vendors regarding the operation-related needs of DIR and DIR customers.

The Customer Engagement Office is responsible for managing DIR's relationship with STS customers and communication functions within the STS Multi-sourcing Services Integrator (MSI) contract. This management includes communicating about and training customers on program policies and updates; tracking customer satisfaction; identifying problems and triaging solutions across the program; resolving customers' escalated operational and service delivery issues; and managing service outreach and growth activities. The team reports to DIR's Deputy Executive Director. The Customer Engagement Office is led by the Director of Customer Engagement and includes six Customer Engagement Managers who primarily support the STS while also helping DIR customers navigate STS offerings.

The STS Financial Analysis team is responsible for the financial oversight of the STS operations. The team is part of the Chief Financial Office and includes the Director of STS Financial Analysis and five employees. The team's duties include managing STS invoicing and balances, forecasting and recommending fee structures to the DIR Board of Directors, and producing STS customer Legislative Appropriations Request (LAR) forecasting and Legislative Budget Board reporting.

The STS Contract Management team is responsible for monitoring and managing contracts between DIR and STS vendors and is part of the Chief Procurement Office. The STS Contract Management team includes the Director of STS Contracts, who oversees five Contract Administration Managers. STS' Contract Administration Managers are ultimately responsible for managing the STS contracts, including facilitating any necessary amendments or work changes to the contracts and managing contractual tasks to address vendor failure to perform or unsatisfactory vendor performance.

The administration of the STS programs also includes STS' contracted Multi-sourcing Services Integrator (MSI). The MSI responsibilities include service-level management, service desk support, constituent helpdesk support, program management, disaster recovery testing and planning, a centralized marketplace, performance analytics, and financial management. DIR's COO oversees the relationship between DIR and this contracted vendor to ensure customer

satisfaction.

STS Processes

DIR utilizes an operational governance framework to address STS issues requiring leadership decision making or alignment within DIR. STS has established hundreds of processes to continue its successful operation. General processes are addressed below.

Procurement and Contract Management

The process for procurement and contract management for the STS is part of the IT Procurement and Contracting function, including appropriate DIR employee participation on the Source Evaluation Board, Source Selection Authority, and the Operational Governance Board. These processes are further described in Section VII. IT Procurement and Contracting.

Governance Models

DIR utilizes an operational governance framework to address STS issues requiring leadership decision making or alignment within DIR.

DIR manages the STS and vendors through two governance models:

- DIR Operational Governance: DIR's internal operational management; and
- STS Owner-Operator Governance: DIR's external governance for customers and vendors.

STS Operational Governance Model

The purpose of the operational governance framework is to gain consensus from the appropriate divisions within DIR when an operation, transition, financial, legal, security, data privacy, or contractual decision needs to be made as part of delivering STS programs to DIR's customer base. The framework offers a forum to share STS information with the broader DIR organization.

Operational governance consists of two levels of oversight and decision making: the Operational Governance Board (OGB) and the Operational Governance Authority (OGA). COO establishes OGB program meetings for the Texas.gov, Data Center Services (DCS), and Managed Security Services (MSS) programs.

The purpose of the OGB is to provide DIR program stakeholders insight into program services and operational issues. The OGB will attempt to obtain consensus from participant stakeholders to make a decision, and, if a consensus cannot be reached, the three designated voting members from the Chief Technology Office (CTO), the Chief Procurement Office (CPO), and the COO will vote. If a decision still cannot be made, the OGB will escalate the issue to the OGA for a decision. The OGA includes DIR's Chief Operations Officer, Chief Technology Officer, Chief Procurement Officer, Chief Financial Officer, and the Chief Information Security Officer.

STS Owner-Operator Governance Model

The STS owner-operator governance model involves DIR and STS customers at all levels in

governance decision making, including as representatives on all governance committees. The model focuses on resolving customer concerns at the lowest possible level and driving for consensus-based solutions involving the service component providers for STS programs and the MSI. Where consensus cannot be reached, escalation processes are in place.

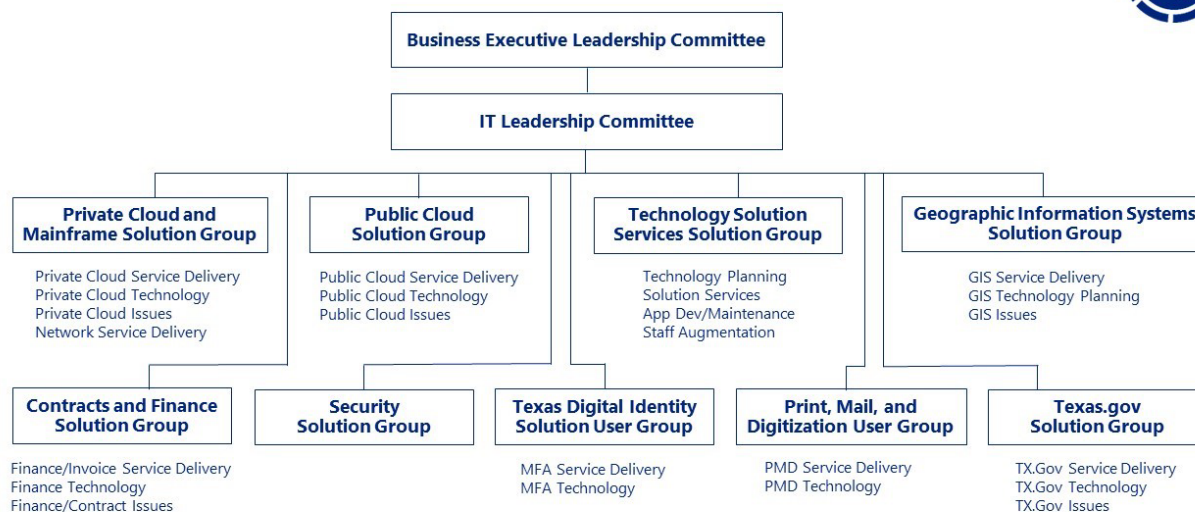
The owner-operator governance model is a set of defined interactions, expectations, decisions, roles, and processes that guide the governance of the programs within STS. The model is designed to facilitate effective resolution of issues and enable strategic decision making; it actively involves DIR and STS customers as full members of solution groups, and the MSI and Service Component Provider (SCP) as associate members. DIR establishes membership based upon the following principles:

- Establish STS customer business executives as leaders in guiding program strategy;
- Implement a decision-making model with STS customer authority and accountability;
- Resolve issues at the lowest possible organizational level;
- Establish representative groups to resolve issues; and
- Formalize roles and responsibilities for strategy and issue management among DIR, STS customers, the MSI, and SCPs.

Owner-operator governance operates at three levels: DIR customer meetings, partner group meetings, and enterprise governance meetings. This governance overview summarizes the owner-operator governance model and provides details concerning enterprise governance committees and solution groups.

Figure 78 STS Governance Framework

STS Governance Framework



Standing governance committees—organized by service and comprised of representatives from STS customers, DIR management, MSI management, SCP management, and subject–

matter experts—carry out decisions and resolve escalated issues. STS customers are structured into partner groups to ensure representation across these committees. Partner groups meet periodically to identify and discuss issues or ideas to bring to governance committees and solution groups for consideration.

In this model, DIR's role includes sustaining governance processes and promoting effective communication. DIR participates as a chair or co-chair on all governance committees, dependent upon the committee's charter, and is responsible for coordinating topics spanning multiple groups and facilitating decision-making.

All SCPs and the MSI participate as required by the governance group charters to identify technical options for solving issues, participate in collaborative solution development, and provide their technical and business perspective.

Data Center Services Program Exemptions

[Government Code Section 2054.391](#) requires state agencies designated for the DCS program to use DCS unless DIR approves a Data Center Services Exemption.²⁹³

To apply for exemption within the Data Center Services program, an agency must submit the following to DIR:

- A cover letter in the form of an executive summary; and
- A completed [Agency Certification Form](#) (available on DIR's website) with required documentation attached. The affirmations and documentation required by this form assure the proposed agency alternative to the Data Center Services-provided service:
 - Is financially viable;
 - Protects agency data;
 - Is in the best interests of the State of Texas; and
 - Ensures hardware and software technical currency.

DIR responds in writing to exemption requests within 30 calendar days of receipt of the request.

DIR processes the following types of Data Center Services Exemptions: infrastructure hosting and Software-as-a-Service (SaaS).

Infrastructure Hosting

Agencies designated by DIR to receive DCS services must request that DIR approve a DCS program exemption before they can procure any infrastructure or infrastructure services outside of the DCS program.

²⁹³ [Gov't Code § 2054.391](#).

Software-as-a-Service (SaaS)

Agencies are required by administrative rule²⁹⁴ to procure any SaaS product with an interface or connection to the DCS system environment through the DCS program, unless an exemption has been requested and approved by DIR.

In addition, the above infrastructure hosting requirements apply to designated agencies purchasing SaaS products that do not interface with DCS environments. Designated agencies are required to seek an approved DCS exemption for any SaaS product procured outside DCS.

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

STS operates as a cost recovery program under [Government Code Chapter 2054 Subchapter L](#).²⁹⁵ DIR customers execute an interagency or interlocal contract agreeing to pay DIR applicable charges for services received from the contractors and the MSI in addition to DIR's recovery fee of 2.95 percent (lowered to 2.75 percent in fiscal year 2024), any allocated charges, and any pass-through expenses incurred. The MSI (Capgemini) administers the STS invoicing and chargeback process, which includes costs incurred by MSI, service component providers, and customers. Each month, the MSI provides SCP and customer invoices to DIR. DIR reviews and approves the costs identified by the invoicing process and sends invoices to customers. After customers pay DIR, DIR pays SCP vendors. DIR does not have visibility into the customer specific funding sources used to pay STS services. STS funding includes interagency contracts and appropriated receipts.

Strategy	Method of Finance	Amount
B.2.1 - DCS	Statewide Technology Account	\$408,593,134

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

DIR's Cooperative Contracts program (COOP) offers contract vehicles for STS' discretionary customers to build and manage their own IT solutions. COOP also provides contract vehicles for customers to manage their own application development, maintenance, and security. COOP is considered more of a "do it yourself" model wherein the customer builds, maintains, and supports their own solutions instead of using STS, which provides an outsourced managed

²⁹⁴ [1 Tex. Admin. Code § 215.43\(a\)\(1\).](#)

²⁹⁵ [Gov't Code Chapter 2054, Subchapter L.](#)

service that allows customers to share already developed technologies and services with established service level attainment requirements and vendor management.

STS and COOP complement each other in many circumstances. For example, COOP eligible entities can use a COOP Deliverable-Based IT Services contract to procure application services that are hosted on DCS compute.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

DIR coordinates customer outreach to ensure that customers understand the difference between COOP and STS, and how to use each program by leveraging the MSI. The objective of the MSI Outreach and Growth management process is to raise awareness about STS to all eligible entities. The MSI coordinates activities with DIR to avoid duplication and ensure consistent messaging.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

Entities must sign an interlocal contract with DIR to receive STS services. The following local and regional entities are eligible for services DIR provides, including programs within the Shared Technology Services function:²⁹⁶

- Local governments, including counties, municipalities, school districts, and junior college districts;²⁹⁷
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and

²⁹⁶ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

²⁹⁷ [Gov't Code § 2054.003\(9\)](#).

- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.²⁹⁸

k) If contracted expenditures are made through this program please provide:

A Short Summary of The General Purpose of Those Contracts Overall

The purpose of the contracts in this program is to deliver STS to DIR Customers.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$406 million in contracted expenditures, the majority of which were funds expended for services consumed by and billed to DIR customers.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 26 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from October 2017 through August 2022 for these contracts. The contracts are funded through amounts billed to and collected from customers and deposited into the statewide technology account.

The Method Used to Procure Those Contracts

These contracts were procured competitively through request for offers, request for quote, and TXSmartbuy.

²⁹⁸ [Gov't Code § 2157.068\(j\); see also Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\).](#)

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-PCM-MSA-436	Rackspace US, Inc.	Public Cloud Manager for the shared technology services.	\$113,521,899.60
DIR-TSS-MSA-435	Deloitte Consulting LLP	Technology Solutions Services provider for shared technology services.	\$100,414,307.24
DIR-TPC-MSA-432	Atos Governmental IT Outsourcing Services, LLC	Private Cloud provider for shared technology services.	\$95,666,475.29
DIR-MF-MSA-439	Atos Governmental IT Outsourcing Services, LLC	Mainframe Services provider for shared technology services.	\$27,553,103.43
DIR-ESS-MSI-407	Capgemini America Inc.	Multi-Services Sourcing Integrator for shared technology services.	\$22,815,318.21

The Methods Used to Ensure Accountability for Funding and Performance

DIR's contract and vendor management processes ensure that contractors perform in accordance with all contractual requirements. Active management of service level agreements also ensures that vendors deliver in accordance with each contract.

A Short Description of Any Current Contracting Problems

Many of the STS contracts have the same initial term and optional renewal dates, which presents certain risks for DIR, STS customers, and the state. To mitigate these risks, DIR sequenced the solicitations, awards, and implementations for the next generation of STS contracts such that we will begin procuring a select few of the STS contracts each year based on the overall best value to the state instead of conducting all procurements simultaneously.

Even with this intentional sequencing, however, there are certain unique challenges associated with the procurement of these large, advanced technology contacts. Most prominent among these is the need for DIR, potential vendors, and STS customers to understand the direction of technological advances, business models, and the market several years in advance of contract award and implementation. DIR begins its market research at least a year prior to the release of the procurement; a given STS procurement can take at least two years to complete. STS contracts usually have a base term of four years with optional extensions totaling up to four years if DIR invokes the optional extension terms. Given this timeframe, DIR conducts market research up to a decade before the conclusion of the contract, which presents challenges for the STS contracts to be flexible in the face of technological innovation.

These contracts also experience challenges associated with competition due to the often-limited number of vendors in the market for these services. To alleviate these concerns, DIR prepares the market for the upcoming procurement using extensive market engagement aimed at making vendors aware of the upcoming procurement and mitigating actual or perceived potential incumbent advantage. At all times, DIR seeks to increase competition for these

procurements and ensure the solicitation is written to promote competition.

DIR also faces procurement challenges due to limited resources with the required expert knowledge and availability. To supplement its resources, DIR often uses a sourcing assistance vendor with additional subject matter experts, procurement project management, and transition assistance for the contract implementation. DIR identifies resource time and availability in the risk matrix and mitigation strategies section of the procurement project management plan for each of the procurements.

l) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

The Texas Legislature adopted [Government Code Chapter 2054 Subchapter L](#), which governs Statewide Technology Centers, in 2005 and has not substantially updated these statutes to reflect the significant changes in technology and industry practices that have occurred in the last 18 years.²⁹⁹ At that time, the technologies being deployed were likely to include software sold through a traditional licensing agreement, often delivered in hard copy, and supported by locally operated infrastructure in a traditional brick-and-mortar data center. As a result, the statute as currently drafted is difficult to apply clearly and unambiguously to technology products and services, which are increasingly delivered solely in a digital format and often supported by cloud-computing infrastructure. Additional flexibility in the language is required if STS is to remain technologically advanced, responsive to customers, and adaptable to the technology offered in the market.

To best position the state to leverage economies of scale and centralized oversight of these new technologies, the subchapter could be amended to reflect how application and infrastructure technologies continue to converge. In particular, the language could be amended to eliminate any ambiguity about whether it applies only to traditional brick and mortar technology centers and to clarify that statewide technology centers include all shared technology services the Legislature deems appropriate for DIR's oversight and operation.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

The following video provides additional information: [Shared Technology Services Overview](#).

²⁹⁹ [Gov't Code Chapter 2054, Subchapter L](#).

o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility). For each regulatory program, if applicable, describe:

While DIR is not a regulatory agency, DIR monitors compliance for the Shared Technology Services function.

Data Center Services Exemptions

Why the Regulation Is Needed

The Legislature expressly desired to create economies of scale and prevent duplicative efforts through the consolidation of data center operations across state government. To ensure achievement of that goal, the Legislature made participation in the DCS program mandatory for all designated DCS customers, and statutorily required those customers to receive DIR's approval prior to procuring any infrastructure hosting or Software-as-a-Service (SaaS) solutions outside of the DCS program. The DCS exemption process is thus needed to effectuate the Legislature's intent for the program.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

Agencies must obtain a DIR-approved exemption prior to entering into any contract or purchase agreement. To apply for exemption of Infrastructure Hosting and SaaS services within the Data Center Services program, an agency must submit each of the following to DIR:

- A cover letter in the form of an executive summary; and
- A completed [Agency Certification Form](#) (available on DIR's website) with required documentation attached. The affirmations and documentation required by this form assure the proposed agency alternative to the Data Center Services provided service:
 - Is financially viable;
 - Protects agency data;
 - Is in the best interests of the State of Texas; and
 - Ensures hardware and software technical currency.

DIR will respond in writing to exemption requests within 30 calendar days of receipt of the request.

Follow-up Activities Conducted When Non-compliance Is Identified

DIR is required by Government Code Section 2054.391(b) to notify the customer agency, the Texas Comptroller of Public Accounts, the Legislative Budget Board, and the State Auditor's Office any time that DIR "becomes aware that a state agency is not using a statewide technology center for operations or services in accordance with the interagency contract entered into under Section 2054.386 and as directed by [DIR]."

Actions Available to the Agency to Ensure Compliance

A state agency may not spend appropriated money for operations or services the agency was

selected to receive through a DIR statewide technology center without the prior approval of DIR's Executive Director.³⁰⁰ The Executive Director of DIR is authorized by Government Code Section 2054.391(c) to approve the expenditure of funds for the services in question after the notice required by Section 2054.391(b) has been provided to all required parties.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Technology Guidance and Innovation



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by **leading the state's technology strategy**, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.

a) Provide the following information at the beginning of each program description.

Name of Program or Function: Technology Guidance and Innovation

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Steve Pier, Deputy Executive Director and John Hoffman, Chief Technology Officer

Statutory Citation for Program:

[Government Code 2054 Subchapter C, General Powers and Duties of Department](#)

[Government Code 2054 Subchapter D, Information Resources Managers](#)

[Government Code Chapter 2054, Subchapter E Strategic and Operating Plans; Information Resources Deployment Review](#)

[Government Code Chapter 2054, Subchapter G, Project Management Practices](#)

[Government Code 2054 Subchapter J, Texas Project Delivery Framework](#)

[Government Code 2054 Subchapter M, Access to Electronic and Information Resources by Individuals with Disabilities](#)

[Government Code Chapter 2054, Subchapter Q, Legacy System Modernization Strategy](#)

[Government Code Chapter 2054, Subchapter R, Information Resources of Government Entities](#)

³⁰⁰ [Gov't Code § 2154.391\(b\).](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.



The objective of the Technology Guidance and Innovative function is to guide state agencies' policies and practices for the effective, efficient use and management of state IT resources.

DIR provides guidance, planning, and reporting on statewide IT priorities. DIR coordinates several statewide programs to advance the use of industry best practices and innovative technologies.

The Technology Guidance and Innovation function is achieved through a variety of major activities classified into three areas:

- Statewide Technology Guidance;
- Information Resources Project Planning and Tools; and
- Innovation and Modernization.

Statewide Technology Guidance

DIR leads the state's technology strategy by working with state IT leaders to establish, track, and report strategic priorities; offer technology education, training, and outreach; and help state agencies make government services, websites, and technology accessible to every Texan.

DIR performs the following Statewide Technology Guidance major activities:

- **Establishing, tracking, and reporting on strategic priorities.** DIR helps set the state's strategic IT priorities by establishing statewide strategic IT goals in the [State Strategic Plan for Information Resources Management](#) through a multi-agency strategic planning process.³⁰¹ DIR assesses statewide progress, reviews agency IT deployment, analyzes statewide IT expenditures, evaluates agency IT infrastructure risks, and confirms compliance with state IT-related statutes and rules.³⁰² DIR reports progress toward statewide IT goals and makes recommendations for statewide IT improvements in the [Biennial Performance Report](#)³⁰³ and additional reports required by statute.³⁰⁴

³⁰¹ [Gov't Code §§ 2054.091-094.](#)

³⁰² [Gov't Code §§ 2054.068](#) and [2054.097.](#)

³⁰³ [Gov't Code § 2054.055.](#)

³⁰⁴ [Gov't Code §§ 2054.157, 2054.260, 2059.057, 2157.007.](#)

- **Providing technology education, training, and outreach.** DIR offers education, outreach, and training to DIR stakeholders.³⁰⁵ DIR assists 143 Information Resources Managers (IRMs) representing 175 agencies by administering the IRM designation and onboarding process, publishing standards in the [Continuing Education Guide for State Agency Information Resources Managers](#), and providing support for meeting continuing education requirements.³⁰⁶ DIR also hosts and co-hosts major conferences, produces webinars, and offers other online or in-person learning and collaboration events.³⁰⁷
- **Administering the statewide digital accessibility program.** DIR oversees a statewide program to help state agencies make Texas government websites, IT, and technology services accessible to every Texan.³⁰⁸ DIR sets statewide policy for electronic and information resources (EIR) accessibility, shares best practices, collaborates with stakeholders, offers tools and resources, and provides guidance to vendors on improving the accessibility of technology products and services for Texas public sector entities.³⁰⁹ DIR provides a robust online accessibility training academy at no charge to employees of state agencies and state-funded institutions of higher education in addition to offering training to vendors responding to solicitations.³¹⁰ In addition, DIR supports agencies and institutions of higher education in meeting EIR accessibility compliance requirements.³¹¹

Information Resources Project Planning and Tools

To keep large technology projects on schedule and on budget, state law requires state agencies to follow the Texas Project Delivery Framework,³¹² which defines how state agencies must manage and implement³¹³ major information resources projects (MIRPs). The Quality

³⁰⁵ [Gov't Code § 2054.051\(c\)](#).

³⁰⁶ [Gov't Code § 2054.076](#).

³⁰⁷ [Gov't Code § 2054.051\(c\)](#).

³⁰⁸ [Gov't Code Chapter 2054, Subchapter M](#).

³⁰⁹ [Gov't Code §§ 2054.452-2054.454](#).

³¹⁰ *Id.*

³¹¹ *Id.*

³¹² [Gov't Code Chapter 2054, Subchapter J](#).

³¹³ [Gov't Code § 2054.003](#) defines "major information resources project" as (A) any information resources technology project identified in a state agency's biennial operating plan whose development costs exceed \$5 million and that: (i) requires one year or longer to reach operations status; (ii) involves more than one state agency; or (iii) substantially alters work methods of state agency staff or the delivery of services to clients; and (B) any information resources technology project designated by the Legislature in the General Appropriations Act as a major information resources project. ** [General Appropriations Act, 87th Leg., R.S., ch. 1053 \(S.B. 1\), Art. IX § 9.07\(d\)](#). Any application remediation project related to Data Center Services (DCS) is also defined as a MIRP, regardless of dollar amount.

Assurance Team ³¹⁴(QAT), composed of DIR, the Texas Comptroller of Public Accounts, State Auditor's Office, and Legislative Budget Board, is charged with monitoring and overseeing those projects. DIR helps agencies follow the framework, collaborates with the QAT on project delivery initiatives, and helps identify enterprise technology sourcing opportunities.

DIR performs the following Information Resources Project Planning and Tools major activities:

- **Providing guidance on major information resources projects.** DIR provides project management, governance, and agile methodology guidance, and conducts regular outreach and educational services to assist agencies and institutions of higher education in IT project governance and management strategies. DIR constantly monitors trends to ensure that strategies and methods provide maximum value to the state.
- **Collaborating with QAT to monitor IT projects.** DIR coordinates and consults with QAT on project delivery initiatives and contracting standards for information resources technologies acquisition and purchased services. In consultation with QAT as well as the Information Technology Council for Higher Education (ITCHE), DIR reviews existing statutes, procedures, data, and organizational structures to identify opportunities to increase efficiency, customer service, and transparency in information resources technologies. DIR maintains the Statewide Project Reporting Application (SPAR) wherein all state agencies report the project status on major information resources projects. DIR uses information that agencies submit to the SPAR to conduct analysis and reporting on the project status information provided to determine an individual project's risk. DIR leads the production, review, revision, and publishing of QAT performance metrics each quarter on the [QAT dashboard](#).
- **Identifying strategic sourcing opportunities.** DIR consults with DIR's agency leadership and customers to identify sourcing opportunities and solutions in DIR's Shared Technology Services (STS) program and Cooperative Contracts program. DIR engages in research and analysis to satisfy its statutory obligation to "provide the leadership in and coordination of information resources management within state government" and "monitor national and international standards relating to information resources technologies."³¹⁵ This research and analysis also aides DIR in: its management of the Cooperative Contracts program;³¹⁶ its operation of statewide technology centers;³¹⁷ and its carrying out of responsibilities under various other statutes by identifying the technologies that might be necessary or useful to state

³¹⁴ [Gov't Code § 2054.158](#).

³¹⁵ [Gov't Code § 2054.051\(a\), \(b\)](#).

³¹⁶ [Gov't Code § 2157.068\(b\)](#).

³¹⁷ [Gov't Code § 2054.376](#).

entities as they serve Texans in the future. DIR's use of strategic sourcing methods is expressly recognized in the [State of Texas Procurement and Contract Management Guide](#).³¹⁸

Innovation and Modernization

DIR works with state agencies to advance digital transformation and cloud adoption, promote technology efficiencies, and increase readiness for the use of advanced technologies. DIR creates collaboration opportunities for digital services and emerging technologies through workgroups and centers of excellence.

DIR performs the following innovation and modernization major activities:

- **Guiding digital transformation.**³¹⁹ DIR assists with digital transformation by offering a [Digital Transformation Toolkit](#) that provides guiding principles to state agencies in their transformation journey. The Strategic Digital Services team provides workshops for agencies to assess and optimize digital transformation capabilities as well as identify and develop digital champions.
- **Prioritizing cybersecurity and legacy systems projects.**³²⁰ DIR analyzes state agency cybersecurity projects and efforts to modernize or replace legacy systems every even-numbered year and makes recommendations to guide state leadership in funding decisions during the appropriations process. In the 2022 **Prioritization of Cybersecurity and Legacy Systems** (PCLS) report, 32 agencies submitted 95 projects with a collective project value of nearly \$927 million.
- **Providing guidance for Application Portfolio Management (APM).** DIR provides a centralized approach for collecting the various attributes of all business applications deployed within an agency, empowering end users to make informed, prioritized investment and risk decisions in the delivery of secure technology services that will better support their core business needs.
- **Providing tools to support the statewide legacy modernization strategy.** DIR provides guidelines, principles, best practices, and references for business and IT professionals developing a plan to modernize a legacy environment. DIR provides engagement advisory support and a series of legacy modernization workshops. DIR provides these services to small agencies with limited infrastructure and resources; they include solution architecture guidance, mentoring, and promotion of enterprise architecture practices. The Application Development Decision Framework helps Texas agencies to develop their next-generation applications.

³¹⁸ Pub. # 96-1809, Texas Procurement and Contract Management Guide 10-11 (2022).

³¹⁹ [Gov't Code § 2054.0691](#).

³²⁰ [Gov't Code § 2054.069](#).

- **Hosting the Texas Artificial Intelligence Center of Excellence (AI-CoE).** DIR assists customer organizations in exploring artificial intelligence (AI) technologies to foster digital transformation. The primary objective of the AI-CoE is to educate and promote emerging AI technologies to improve the delivery of government services to Texans in a secure and efficient manner.
- **Collaborating through the Cloud Center of Excellence (Cloud CoE).** DIR collaborates with stakeholders to accelerate cloud adoption, establish a new mindset to think “cloud first” and “cloud smart” for new applications, and reduce technology maintenance overhead. The Cloud CoE trains agency employees in solutions using real-life use cases.

c) What information can you provide that shows the effectiveness and efficiency of this program or function? If applicable, reference but do not repeat any performance measures from Section II, Exhibit 2, and provide any other metrics of program effectiveness and efficiency. Also, please provide the calculation or methodology behind each statistic or performance measures.

DIR measures effectiveness and efficiency of the Technology Guidance and Innovation function through a variety of metrics. The effectiveness of this function is gauged from the engagement of customer agencies in the programs and services offered through this group.

DIR publishes planning and reporting documents on its website and the Texas Open Data Portal. As of July 2023, over 2,400 visitors have accessed the 2022-2026 State Strategic Plan for Information Resources Management and the 2022 Biennial Performance Report online or through the portal.

DIR provides training to state agency IRMs to assist them in meeting continuing education requirements, including hosting 51 education programs in FY22, with 97 percent of those attending rating the events favorably as detailed by the chart below.

Figure 79 FY22 Continuing Education Events

FY22 Continuing Education Events			
Type of Event	Number of Events Held	Total Number of Attendees	Percentage of Favorable Evaluations
DIR Hosted or Co-hosted Events	23	1,524	95.71%
DIR's Technology Today Series	11	789	97.17%
DIR-Promoted Events	17	785	100.00%
Total for All FY22 Continuing Education Events	51	3,098	96.68%

DIR supports state agencies and institutions of higher education to provide Texas government

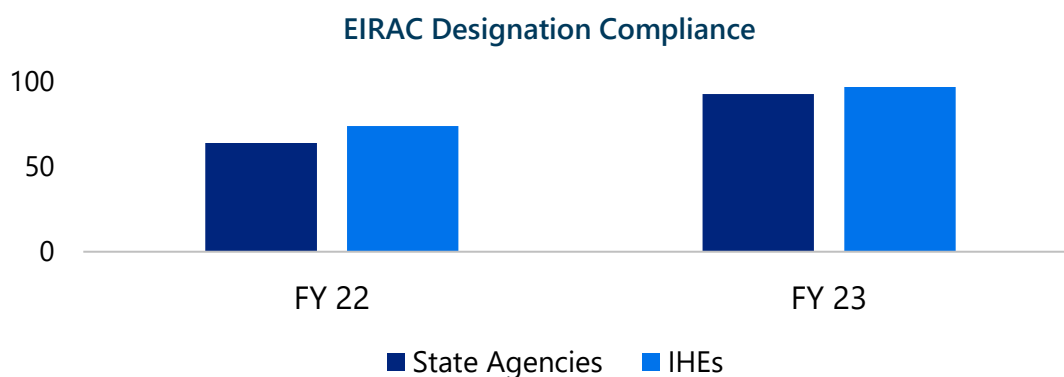
websites, IT, and technology services that are accessible to every Texan. DIR is required to provide digital accessibility training and technical assistance to state agencies, and DIR satisfies this requirement by offering state agencies and institutions of higher education free access to Access Academy, a digital accessibility learning management system. In 2023, 290 state employees registered for Access Academy accounts. Additionally, DIR provides training for vendors on Texas procurement compliance for digital accessibility.

As of June 30, 2023, the digital accessibility program metrics show DIR:

- Conducted 123 outreach activities in FY22, and 172 in FY23, including presenting or sharing resources at statewide monthly meetings, lunch and learns, and conferences;
- Facilitated the scanning of 17 state of Texas websites for accessibility compliance; and
- Onboarded 44 new EIRACs in FY23.

State agencies and institutions of higher education are required by 1 Texas Administrative Code (TAC) 213.21(a) and TAC 213.41(a) to appoint an Electronic and Information Resources Accessibility Coordinator (EIRAC), which provides leadership and guidance, ensures compliance, and promotes EIR accessibility in their organization. From 2022 to 2023, state agencies' compliance with the EIRAC designation requirement increased 29 percent, to 93 percent of state agencies compliant with the requirement. Compliance among institutions of higher education increased 23 percent, to 97 percent compliant in 2023.

Figure 80 EIRAC Designation Compliance



d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

1989

The Legislature passed the Information Resources Management Act and created DIR with statewide information resource planning and reporting activities as a core function. The primary

purpose and objectives for planning remain focused on the efficient and effective use of technology across state government.

2005

EIR accessibility in the state was strengthened when the 79th Legislature required state agencies to ensure that their electronic information technology is accessible to citizens with disabilities, including state employees. DIR developed an enterprise level accessibility strategy to provide state agencies with access to tools and guidance needed to comply with state and federal regulations.

The 79th Legislature (2005) adopted [House Bill 1516](#), which requires the use of the Texas Project Delivery Framework (Framework).³²¹ Effective September 1, 2005, state agencies and institutions of higher education (collectively referred to as agencies) are required to use the Framework for delivery of all major information resources projects. DIR, in collaboration with other agencies, the Legislative Budget Board, State Auditor's Office, [Quality Assurance Team](#) (QAT), and other stakeholders developed and published an initial Framework baseline.

2007

The 80th Legislature made several changes to the agency information reporting process to streamline and align the planning, reporting, and review of the state's information resources. Chief among these was dividing the information resources strategic plan into two more meaningful reports—the Information Resources Deployment Review and a new information resources component of the agency strategic plan.

2019

DIR created the Cloud Center of Excellence (CoE) following legislative direction to advance Texas state agencies' use of cloud services. Driving education and hands-on experience in this modern technology provided a foundation for technology teams to leverage cloud solutions. Thousands of training events have occurred in partnership with expertise from more mature entities and the marketplace, including all areas of responsibility within agencies such as finance, legal, procurement, security, and IT. DIR created much-needed awareness of the technology to foster adoption.

2020

With the success of Cloud CoE, DIR replicated the model to create the AI-CoE to accelerate innovation and adoption of AI technologies, such as machine learning, robotic process automation, and natural language processing. The AI-CoE helps state and local governments and public institutions of higher education explore AI technologies to foster digital

³²¹ [Acts 2005, 79th Leg., R.S., ch. 1068 \(H.B. 1516\), § 1.06, 2005 Tex. Sess. Law Serv. 3544, 3545 \(codified at Gov't Code Chapter 2054, Subchapter J\).](#)

transformation.

2021

During the 87th Regular Legislative Session, the Legislature passed [HB 1576](#) that created the Work Group on Blockchain Matters.³²² The Work Group consisted of 16 appointed members, including a representative from DIR appointed by the Governor. The bill tasked the group with developing a master plan for the expansion of the blockchain industry in Texas and to recommend policies and state investments in connection with blockchain technology.

The Work Group began meeting monthly in December 2021 and had seven areas of study including Commercial Law and Contracts, Digital Identity, Decentralized Autonomous Organizations, Energy, Finance, Government Use Cases and Official Record keeping systems.

2022

Throughout 2022, the seven subcommittees researched the current state of blockchain in Texas and held two public hearings. DIR participated in the 'Government Use Cases' subcommittee which was tasked with identifying government use cases for blockchain. In November 2022, the group produced the 2022 Texas Work Group on Blockchain Matters [report](#) and proposed master plan to expand the blockchain industry in Texas, as required by HB 1576. DIR currently serves as a resource for agencies interested in blockchain technology for solving specific use cases.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The Technology Guidance and Innovative function's services and programs are available for the public sector to use as a resource for strategic technology planning, digital accessibility, and project management. The following entities are eligible for services DIR provides, including programs within the Technology Guidance and Innovation function:³²³

- State agencies;
- Local government organizations;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;

³²² [Acts 2021, 87th Leg., R.S., ch. 320 \(H.B. 1576\), § 1.](#)

³²³ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

- Public hospitals owned or operated by this state, or a political subdivision or municipal corporation of this state including a hospital district or hospital authority;
- An independent organization certified under Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Tax Code Section 152.001; and
- Government entities of another state.

f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.

Technology Guidance and Innovation Administration

The Technology Guidance and Innovation function is administered by the Deputy Executive Director and the Chief Technology Officer. The Technology Guidance and Innovation function includes the following activities:

- Planning, Policy, and Reporting;
- IRM Outreach and Digital Accessibility;
- Digital Project Services; and
- Strategic Digital Services.

Planning, Policy, and Reporting

DIR's Planning, Policy, and Reporting activities are administered through the Office of Public Affairs and Strategic Initiatives and the Chief Data Office within the Deputy Executive Director's Office.

The Planning, Policy, and Reporting Program is led by a Director supported by a Policy Analyst, who are part of the Office of Public Affairs and Strategic Initiatives. They are responsible for:

- Establishing, tracking, and reporting on statewide strategic technology priorities;
- Setting statewide strategic IT goals in the State Strategic Plan for Information Resources Management through a multi-agency strategic planning process;
- Assessing statewide progress by reviewing agency IT deployment, analyzing statewide IT expenditures, evaluating agency IT infrastructure risks, and confirming compliance with state IT-related statutes and rules, in addition to reporting progress

towards statewide IT goals and making recommendations for statewide IT improvements in the Biennial Performance Report; and

- Collaborating with stakeholders to produce additional plans, reports, briefings, and guidance as required by statute including the agency strategic plan each biennium.

The Planning, Policy, and Reporting Program is also supported by a Data Analyst who surveys state agencies and provides data analysis for DIR's legislatively required reports. The Strategic Reporting Data Analyst conducts the Information Resources Deployment Review, a biennial self-assessment tool designed to reveal agency's technology strengths and weaknesses and to inform improvements for information resources statewide. The Strategic Reporting Data Analyst is a part of the Chief Data Office.

IRM Outreach and Digital Accessibility

DIR's IRM Outreach and Digital Accessibility activities are administered through the Chief Experience Office within the Deputy Executive Director's Office. These activities increase information sharing among IRMs and provide them with continuing education opportunities. DIR partners with EIRACs to increase state agency and institution of higher education digital accessibility engagement and maturity.

The IRM Education and Outreach Coordinator assists IRMs in meeting their continuing education requirements by coordinating outreach, collaboration, and education opportunities. The IRM Education and Outreach Coordinator produces conferences (hosted and co-hosted by DIR), regular webinars, and other online or in-person learning events for IRMs. The role also reviews and updates IRM designation and continuing education requirements, publishes standards in the [Continuing Education Guide for State Agency Information Resources Managers](#), administers IRM designations and onboarding, and tracks and reports on IRM continuing education compliance. The IRM Education and Outreach Coordinator is a part of the Chief Experience Office.

The Statewide Digital Accessibility Program Administrator administers the statewide digital accessibility program to increase public-sector digital accessibility maturity through providing tools, resources, outreach, and collaboration opportunities to assist vendors' understanding of EIR accessibility compliance requirements. In addition, the Statewide Digital Accessibility Program Administrator improves and standardizes EIR accessibility review criteria for cooperative contract procurements, works to increase vendors' understanding of state EIR accessibility requirements, and offers training to state agency and institution of higher education employees through a robust online training academy. The Statewide Digital Accessibility Program Administrator is a part of the Chief Experience Office.

Digital Project Services

The Digital Project Services activities are administered through the Chief Technology Office by the Director of Strategic Sourcing and a Digital Project Services Project Manager.

The Director of Strategic Sourcing provides direction and guidance on DIR's strategic statewide programs to identify sourcing opportunities in DIR's enterprise solutions and Cooperative

Contracts. The Director establishes the strategic digital plans, goals, and objectives with agencies, IT departments, and senior leaders to align digital technology plans with business goals and leads discovery, research, and analysis for current and new technology services being considered by DIR. The Director also leads the Statewide IT Project Oversight and the Project Delivery Framework program, and oversees staff review of deliverables, the execution of training programs for state agency staff, and program improvement activities. The Director serves as Quality Assurance Team (QAT) liaison for DIR, and as the escalation path for project review and monitoring activities, contract review and evaluation activities, and process improvement activities.

The Digital Project Services Project Manager provides consultative services and technical assistance to enable technological advancement in DIR's enterprise solutions and Cooperative Contracts. The Project Manager also assists in DIR's Texas Project Delivery Framework (TPDF) and the state's QAT programs by reviewing state IT project planning deliverables and status reports; administering DIR's Statewide Project Automated Reporting (SPAR) tool; assisting agency project management and business leaders in completing deliverables in compliance with state laws and rules; participating in analysis, research, and reporting for the programs; and implementing continuous process improvements.

Statewide Project Delivery Framework

DIR continuously identifies and delivers enhancements for the Statewide Project Delivery Framework and statewide project delivery. As part of a continuous process improvement, effective implementation of an advisory board was necessary to ensure that the Framework and statewide project delivery guidance meet the business needs of agencies and institutions of higher education.

The Project Delivery Advisory Board fulfills its purpose primarily by executing the following strategies:

- Implement a standard, repeatable, predictable, and transparent change advisory process.
- Remain focused on statewide business needs based on—and in relation to—individual agency business needs.
- Place greater emphasis and priority on required aspects of the Framework.
- Align with QAT policies and procedures.
- Act in accordance with legislative direction as stipulated in statute.

The Project Delivery Advisory Board comprises nine representatives from specific domains of expertise, institutions of higher education, small state agencies, medium-size agencies, and large-size agencies. Two representatives are from institutions of higher education. Each agency on the Project Delivery Advisory Board is limited to a maximum of two named participants. The Project Delivery Advisory Board meets a minimum of twice a year, though additional meetings may be scheduled on an as-needed basis.

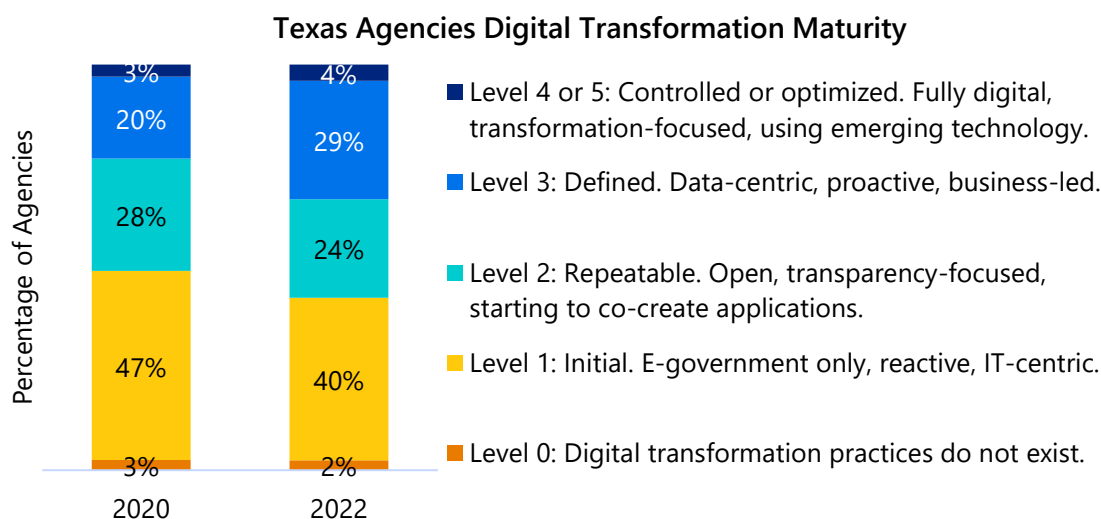
Strategic Digital Services

Lasting digital transformation or modernization requires the integration of the right technology with people, processes, and tools to fundamentally change how the public sector delivers services to Texans in a modern world. According to the [2022 Biennial Performance Report](#), agencies reported that they are making progress on modernizing legacy systems and applications with 22 percent of agencies considering themselves fully modernized; 75 percent of agencies said at least half of their application portfolios are modernized. Issues associated with legacy applications include unavailable software maintenance upgrades, the inability to adapt or enhance software, limited expertise, and insufficient technical support and documentation.

Agencies not only understand the urgency of modernizing, but they are also poised to take advantage of the benefits of AI. Over a third of state agencies report they have already deployed some form of AI solutions.

DIR created the Strategic Digital Services (SDS) team to assist agencies in their digital transformation and modernization journey.

Figure 81 Texas Agencies Digital Transformation Maturity



The SDS team, administered through the Chief Technology Office, includes the Deputy Chief Technology Officer, the Director of Strategic Digital Services, and an Enterprise Solutions Architect.

The Deputy Chief Technology Officer reports to the Chief Technology Officer and translates business strategy into digital IT strategies and DIR solutions for state and local agencies. The deputy Chief Technology Officer's goal is to successfully define, advise, and drive digital services that enable state agencies' digital innovation, transition, and efficiencies. The Deputy Chief Technology Officer is responsible for developing the strategy, roadmap, and design—and for being a resource during the implementation—of DIR's portfolio of digital services. The Deputy Chief Technology Officer develops iterative plans and solutions that ensure that digital

technology objectives are aligned with business goals and provides executive briefings, leadership reviews, and staff training on solutions and services.

The Director of Strategic Digital Services develops solutions and establishes goals and objectives to promote digital tools consistent with IT solutions and digital productivity plans. This role provides state agency leaders with an understanding of digitization and its importance for their agency, in addition to leading technical staff from state agencies to drive technical strategies related to digital initiatives and shared goals and solutions.

To assist agencies as a guiding principle in their transformation journey, DIR produced a Digital Transformation Guide and Toolkit available on the DIR website. The Director of Strategic Digital Services oversees the digital transformation toolkit and provides workshops for agencies to assess and optimize digital transformation capabilities as well as identify and develop digital champions. The Director of Strategic Digital Services oversees the AI-CoE, which educates and promotes emerging AI technologies among state agencies to improve the delivery of government services to Texans in a secure and efficient manner.

The Enterprise Solutions Architect is responsible for translating business strategy into IT strategy, analyzing IT systems, and working closely with the technical leaders of state agencies. The Enterprise Solutions Architect develops iterative plans and solutions for customer state agencies that ensure that technology objectives are aligned with business goals. The role also facilitates the Cloud CoE, which provides hands-on training opportunities for government entities and facilitates meetings between cloud providers and agencies to assist them in developing proof-of-concepts and pilot projects.

The SDS team collaborates with the Office of the Chief Information Security Officer (OCISO) to produce the Prioritization of Cybersecurity and Legacy Systems (PCLS) Report every even-numbered year before the start of the Texas Legislative session. Through the PCLS report, DIR summarizes state agency cybersecurity projects and efforts to modernize or replace legacy systems. [Government Code Section 2054.069](#)³²⁴ requires DIR to report on state agency cybersecurity projects and projects to modernize or replace legacy systems, as defined by [Government Code Section 2054.571](#).³²⁵

To develop the required list of prioritized projects, DIR relies on PCLS Project Questionnaires, which provides agencies with the opportunity to demonstrate the risks and potential impacts of appropriations for their cybersecurity and legacy modernization projects. DIR uses the responses provided in the PCLS Project Questionnaires, along with the business applications associated with the project, in determining the project prioritizations that are sent to the Legislative Budget Board.

The SDS team, in collaboration with OCISO: maintains and updates the PCLS Project

³²⁴ [Gov't Code § 2054.069](#).

³²⁵ [Gov't Code § 2054.571](#).

Questionnaires, instructions, and training materials; presents PCLS webinars to agency IRMs; gathers and analyzes the questionnaire data from the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM); and creates the PCLS Legislative Budget Board report, agency report, and PCLS public report.

The SDS team collaborates with the Shared Technology Services (STS) on the Application Portfolio Management (APM) tool, which provides a centralized approach for collecting the various attributes of all business applications deployed within an agency. The APM tool empowers end users to make informed and prioritized investment and risk decisions in the delivery of secure technology services that will better support their core business needs. The APM tool can provide a complete inventory of an agency's business applications and associated resources needed for the operational support of those applications over the application lifetime (such as budget, staff time, and infrastructure). The SDS team and STS coordinate kick-off meetings, provide hands-on workshops, and provide continuous support to STS agencies as they go through the APM tool onboarding phase and beyond. DIR and participating agencies work closely on tool enhancements and process improvements.

The SDS team also provides state agencies with advisory support and legacy modernization workshops.

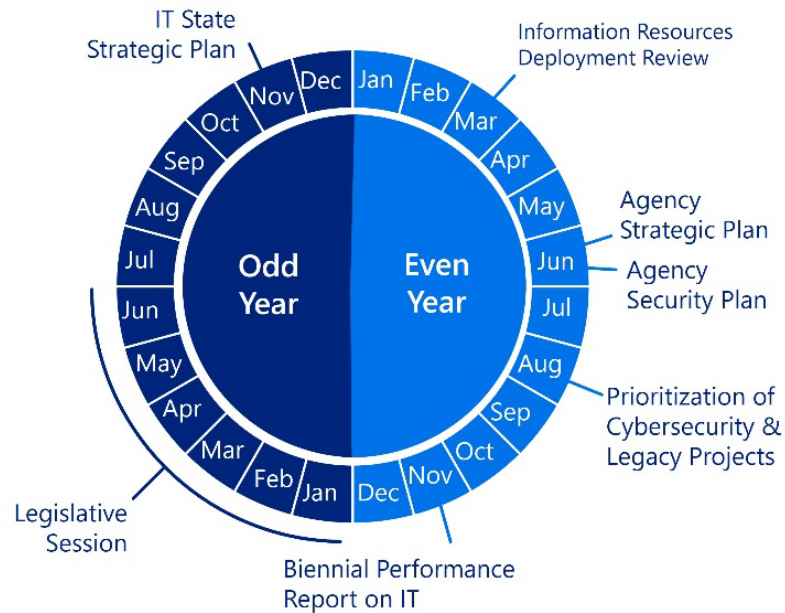
Technology Guidance and Innovation Processes

Planning and Reporting Framework

DIR administers the Planning and Reporting Framework under various statutes.³²⁶ The technology planning and reporting cycle provides a process for strategic thinking and goal setting to ensure that state leadership has the information they need to guide policy decisions. The process of technology planning and reporting involves planning, assessing, acting, and communicating about strategic goals—and the progress made toward achieving those goals. It provides a framework for state agencies to use in setting agency-level technology priorities.

³²⁶ Gov't Code §§ [2054.055](#), [2054.068](#), [2054.091-.097](#).

Figure 82 Planning and Reporting Framework



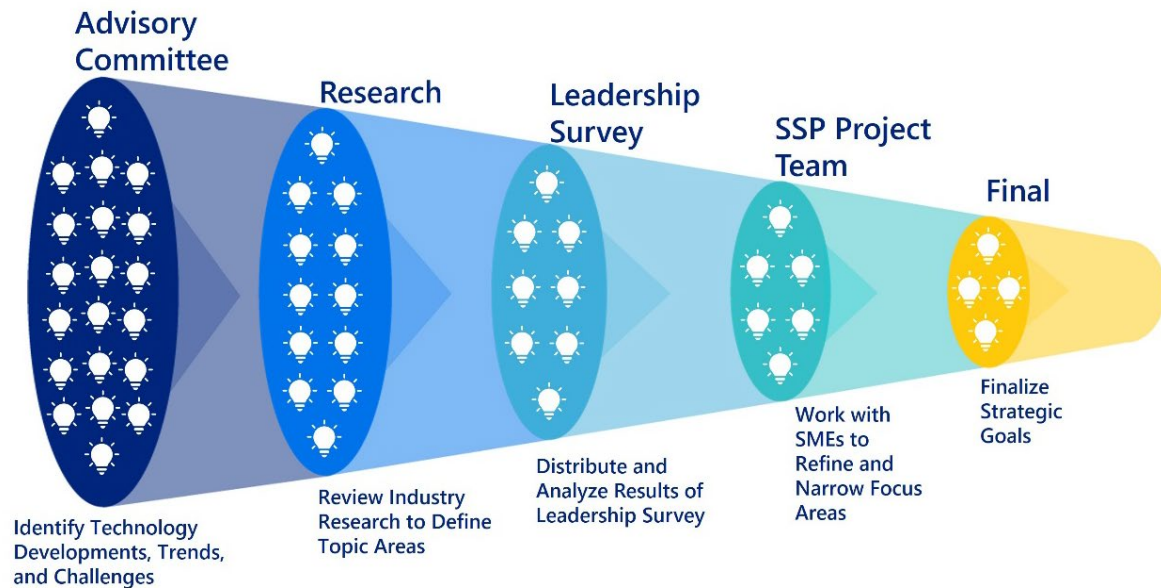
State Strategic Plan Process

In the odd-numbered years, DIR tracks technology legislation and considers the implications on statewide goals. DIR coordinates a strategic planning process and publishes the State Strategic Plan (SSP) for Information Resources Management.

To publish the State Strategic Plan, DIR:

1. Establishes an advisory committee to assist with preparation of the plan.
2. Gathers additional information through industry research, subject matter expert input, and a public-sector leadership survey.
3. Writes, reviews, and produces the plan.
4. Promotes the plan for use by agencies and institutions of higher education.

Figure 83 State Strategic Planning Process



Information Resources Deployment Review Process

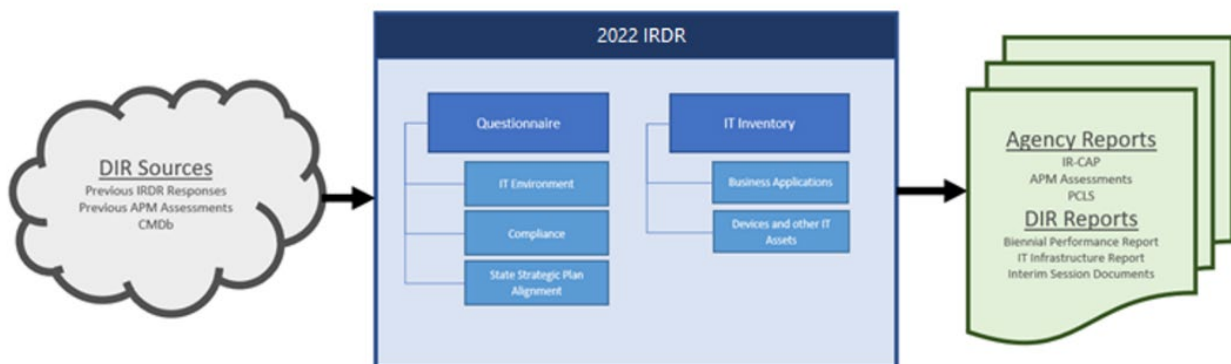
In even-numbered years, DIR coordinates the Information Resources Deployment Review (IRDR).

To coordinate the IRDR, DIR:

1. Develops the IRDR questionnaire, updates SPECTRIM, and publishes instructions.
2. Communicates IRDR reporting requirements to IRMs and helps throughout the process.
3. Evaluates the IRDR results and agency corrective action plans.

DIR uses the IRDR results to prepare the Biennial Performance Report, which informs state leadership on state government's use of information resources technologies.

Figure 84 Information Resources Deployment Review Process



Biennial Performance Report Process

In even-numbered years, DIR uses the information from the IRDR and other sources to produce the Biennial Performance Report and additional supplemental reports.

To produce the Biennial Performance Report, DIR:

1. Analyzes the results of the IRDR, assesses progress toward statewide strategic IT goals, and works with subject matter experts to develop report content.
2. Develops legislative recommendations for improving statewide IT use and management.
3. Writes, edits, and completes the reports.
4. Publishes and distributes the Biennial Performance Report and additional supplemental reports.

Figure 85 Biennial Performance Reporting Requirements

Report Title	Texas Government Code
Biennial Performance Report	Section 2054.055
State Technology Expenditures	Sections 2054.055 (b)(4)
Electronic Information Resources Accessibility	Section 2054.055 (b)(9)
Texas.gov	Sections 2054.055(b)(6)-(7) and 2054.260
Telecommunications Performance	Sections 2054.055(b)(10) and 2054.055 (b-1)
Project Management Practices	Section 2054.157(b)
Internet-Based Training	Section 2054.055 (b)(8)
Cloud Computing	Section 2157.007
IT Infrastructure	Section 2054.068
Consolidated Network Security System	Section 2059.057

IRM Education and Outreach

By both statute and administrative rule, DIR administers the IRM education and outreach functions.³²⁷

IRM Designation and Onboarding

Texas state agencies and institutions of higher education must designate an IRM who is part of their executive team and reports directly to their agency's head or deputy head of operations.³²⁸ DIR verifies compliance with this requirement by requesting an organizational chart that shows the position of the IRM at the time of designation.

DIR manages a record of required state agency and higher education IRMs. DIR reviews IRM qualifications prior to the onboarding of a new IRM to ensure that they comply with requirements. The designation process involves the receipt of an IRM designation letter from the designating agency's head or deputy head of operations. The designation letter must also

³²⁷ [Gov't Code § 2054.051\(c\)](#); [Gov't Code § 2054.076](#); [1 Tex. Admin. Code ch. 211](#).

³²⁸ [Gov't Code § 2054.075](#).

include an organizational chart depicting the IRM's place in their agency structure.

Once their designation has been processed by DIR, the IRM receives an onboarding packet with information on the IRM role, requirements, and responsibilities. DIR holds IRM orientations at least twice a year to communicate this information to recently designated IRMs. DIR documents agency compliance with IRM continuing education requirements on an annual basis.

To designate and onboard IRMs, DIR:

1. Requests that agency heads or their designee provide a letter to DIR designating their agency's IRM.
2. Reviews and approves the designation.
3. Sends an onboarding packet with information on the IRM role, requirements, and responsibilities once an IRM is assigned.
4. Hosts an IRM orientation at least twice a year.

IRM Continuing Education Events

DIR provides educational opportunities to IRMs year-round to assist IRMs with meeting the continuing education requirements of the IRM role. DIR hosts multiple in-person and virtual training events annually. DIR also promotes educational opportunities for IRMs that are hosted by external organizations. All educational events hosted by organizations other than DIR require approval from DIR leadership.

To host an IRM continuing education event, DIR:

1. Determines event dates, location, and format.
2. Coordinates registration, exhibitors (if applicable), speakers, and event logistics.
3. Conducts event day activities.
4. Evaluates the event.

Digital Accessibility Education and Outreach

The Digital Accessibility Program is administered under Government Code 2054 subchapter M. Per administrative rule, DIR provides access to digital accessibility courses for agencies and institutions of higher education.³²⁹ DIR's Statewide Digital Accessibility Program Administrator speaks at conferences, offers training courses on procurements, shares knowledge with agencies and institutions of higher education, and shares information on digital accessibility conferences and webinars outside the statewide program. DIR hosts a monthly Digital Accessibility meetup for state employees. The monthly meetings offer training and forums to discuss issues and provide peer support.

To promote digital accessibility and outreach, DIR:

1. Shares information on the digital accessibility learning management system.
2. Responds to—and registers in the system—state employee and vendor requests.

³²⁹ 1 Tex. Admin. Code §§ [213.19](#), [213.39](#).

3. Audits the learning management system monthly to ensure that only state employees have access.
4. Shares information on monthly live training sessions with the digital accessibility community.

Digital Accessibility Survey

DIR administers a digital accessibility survey through the Information Resources Deployment Review (IRDR) in even-numbered years, including sections for accessibility compliance.³³⁰ DIR reviews the data and shares the survey results in the Biennial Performance Report.

To prepare the accessibility compliance sections of the Biennial Performance Report, DIR:

1. Reviews IRDR survey data for the accessibility sections.
2. Creates data visualizations for the Biennial Performance Report.
3. Reviews and edits the Digital Accessibility section of the Biennial Performance Report.

EIRAC Designation and Onboarding

DIR supports the designation and onboarding of Electronic and Information Resources Accessibility Coordinators (EIRACs), a required role for state agencies and institutions of higher education.³³¹ DIR maintains a list of all state agency and institution of higher education assigned EIRACs and performs a periodic audit to ensure that agencies and institutions of higher education are compliant.

To designate and onboard EIRACs, DIR:

1. Instructs agency heads or IRMs to complete the EIRAC designation form on the DIR website.
2. Reviews and approves the designation on the form.
3. Sends a welcome packet with information on the EIRAC role, requirements, and responsibilities to the newly assigned EIRAC.

Project Delivery Framework

To make project management easier, DIR collaborated with state agencies to create the Project Delivery Framework templates (for major technology projects) and Project Management Essentials templates (for small-to-medium-scale projects under \$5 million). The framework is administered by the Quality Assurance Team (QAT) with templates and guidance (such as the [Texas Project Delivery Framework Reference Guide](#)) to ensure that major projects are planned and managed wisely.³³²

³³⁰ [1 Tex. Admin. Code §§ 213.20, 213.40](#); 1 Tex. Admin. Code §§ [206.50](#), [206.70](#).

³³¹ [1 Tex. Admin. Code §§ 213.21, 213.41](#).

³³² [Gov't Code Chapter 2054, Subchapter J](#).

Digital Transformation Guide

DIR helps Texas government advance digital transformation and improve customer experience, regardless of where the organization is on its digital journey.³³³ The [Digital Transformation Guide](#) recognizes key considerations for digital transformation, outlining a five-step process for advancing the next generation of digitization in Texas government and identifying state resources for public sector organizations to facilitate the digital transformation.

Figure 86 Digital Transformation Process



³³³ [Gov't Code § 2054.0691.](#)

Digital Transformation Tools and Templates

DIR provides Digital Transformation Tools and Templates to assist organizations with their Digital Transformation process. Organizations can use these tools and templates as is, or they can engage DIR to conduct workshops.

Figure 87 Digital Transformation Tools

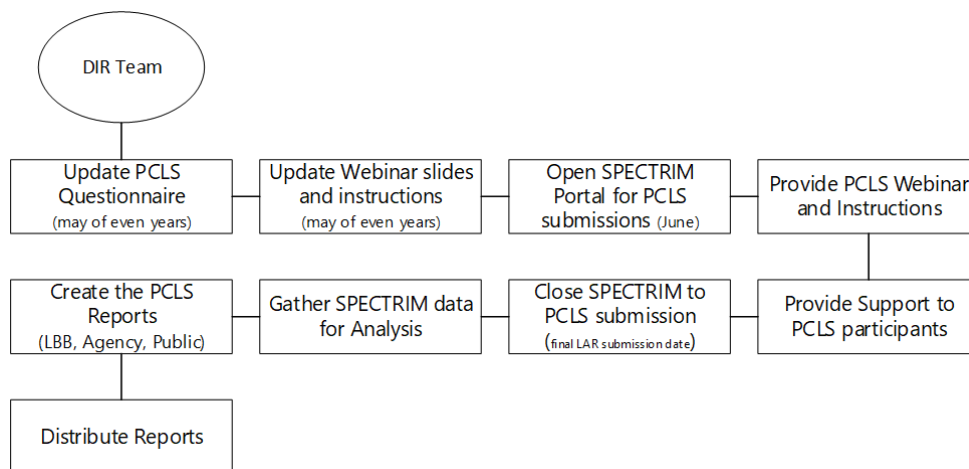


Prioritized Cybersecurity and Legacy Systems Projects Report

[Government Code Section 2054.069](#)³³⁴ requires DIR to report on state agency cybersecurity projects and projects to modernize or replace legacy systems, as defined by [Government Code Section 2054.571](#),³³⁵ to the Legislative Budget Board no later than October 1 of each even-numbered year.

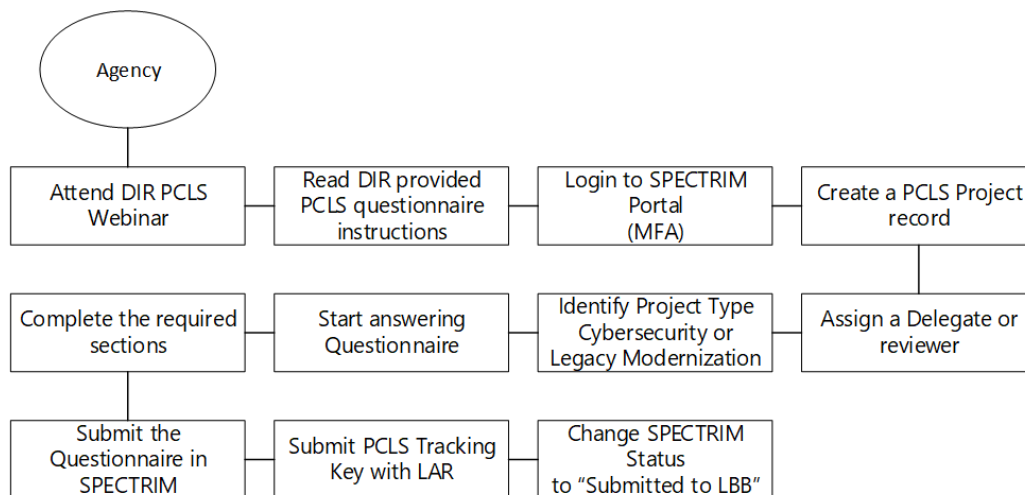
The following flowchart shows the PCLS workflow process for DIR.

Figure 88 PCLS Workflow Process



The following flowchart shows the PCLS workflow process for an agency to create and submit a PCLS project.

Figure 89 Process to Create and Submit a PLCS Project



³³⁴ [Gov't Code § 2054.069](#).

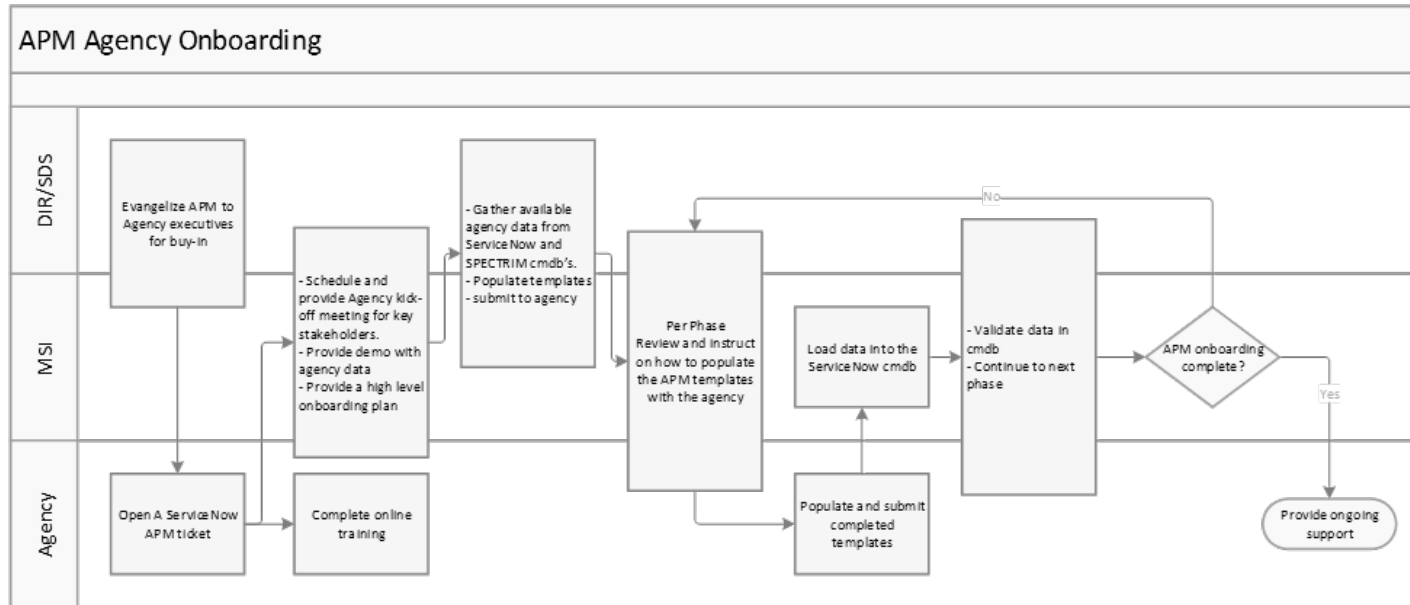
³³⁵ [Gov't Code § 2054.571](#).

Application Portfolio Management (APM)

The APM onboarding process starts with an agency submitting an APM onboarding ticket via the Shared Technology Services program's service catalog request. Working closely with the Multi-sourcing Services Integrator (MSI) and Strategic Digital Services (SDS) teams, the agency is guided through a three-phased approach to APM onboarding.

The following flowchart shows the APM onboarding workflow process.

Figure 90 APM Agency Onboarding

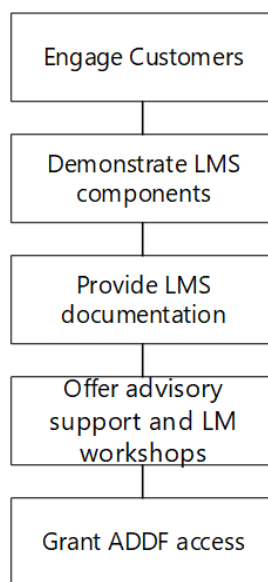


Legacy Modernization Strategy

The Legacy Modernization Strategy (LMS) provides a comprehensive legacy modernization package that agencies can use to conduct, track, and support their legacy modernization initiatives. DIR's LMS process begins with the SDS team engaging with an agency's executives and promoting DIR's supplied artifacts, guides, and tools. Further engagement may involve workshops, advisory support, and documentation that an agency can use to conduct, track, and support their legacy modernization initiatives.

The flowchart below outlines the LMS engagement process.

Figure 91 LMS Engagement Process



Centers of Excellence

Artificial Intelligence Center of Excellence

The Texas Artificial Intelligence Center of Excellence (AI-CoE) was formed to accelerate innovation and secure adoption of artificial intelligence (AI) technologies. Through the center, DIR helps state governments, local governments, and public institutions of higher education explore AI technologies to foster digital transformation.

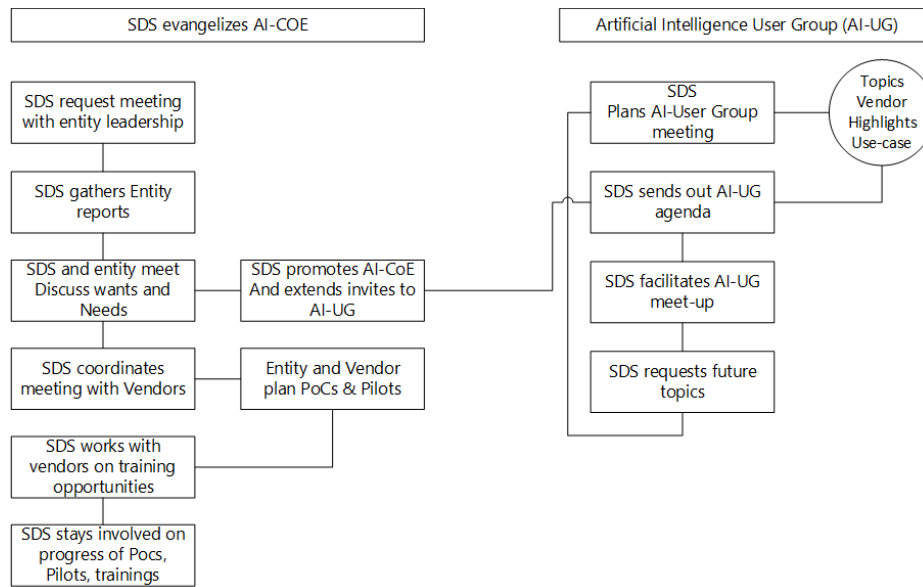
The AI-CoE leverages subject matter experts to educate and assist agencies in adopting technology, exploring AI opportunities, and developing a digital workplace that promotes automation as outlined in the State Strategic Plan. The AI-CoE assists agencies in recognizing and evaluating risks associated with AI, including privacy and security concerns, potential biases, and attribution issues. To limit those risks, the AI-CoE provides collaboration and training on the implementation of AI best practices. This DIR initiative helps customers to identify their needs, engage with the vendors to understand their offerings and services, and facilitate training events and user group communities that showcase use cases and opportunities.

The AI User Group is a community of individuals from state agencies, local governments, and institutions of higher education involved in the day-to-day business and administrative responsibilities of their organization who are looking to incorporate AI into their processes in a secure and ethical manner. DIR facilitates the AI User Group monthly to direct and focus future AI-CoE operations.

The process of the AI-CoE involves direct engagement with agency staff to offer training opportunities or potential AI proofs of concept or pilot initiatives.

The flowchart below outlines the AI-CoE process.

Figure 92 AI-CoE Process



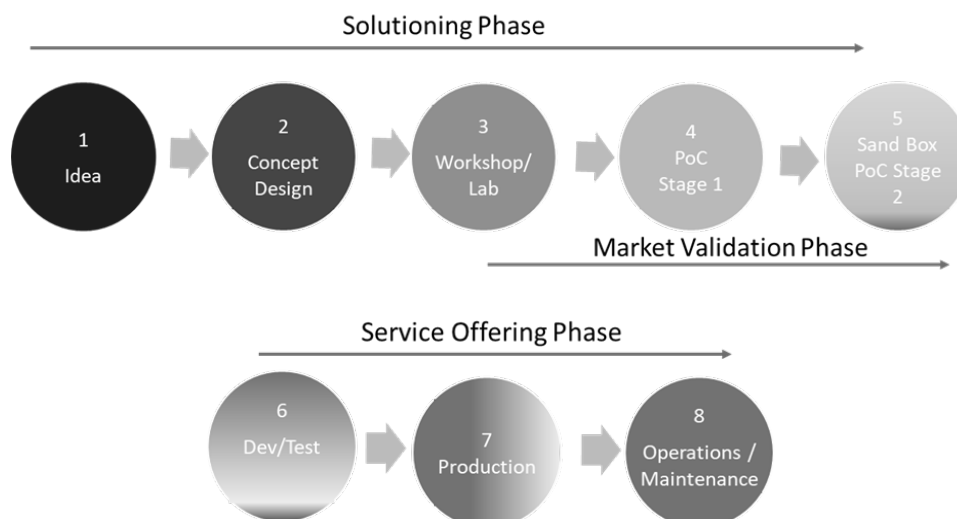
Cloud Center of Excellence

The purpose of the Cloud Center of Excellence (or Cloud CoE—formerly Cloud Tiger Team) is to help accelerate cloud adoption and establish a new mindset to think “cloud first” and “cloud smart” for new applications to reduce technology maintenance overhead.

The Cloud CoE promotes the DIR Proof of Concept Lifecycle Methodology as an approach to customer engagement and cloud adoptions. This methodology is used to determine whether an idea can be turned into a reality. The methodology is meant to determine the feasibility of the idea or to verify that the idea will function as envisioned. The methodology is composed of eight stages across three main phases: Solutioning, Market Validation, and Service Offering.

The methodology is as follows.

Figure 93 DIR Proof of Concept Lifecycle Methodology



g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The funding for the Technology Guidance and Innovation function comes from fees collected from the sale of technology commodities and services through the Cooperative Contracts program.

Strategy	Method of Finance	Amount
A.1.1 – Statewide Planning and Rules	Clearing Fund	\$770,905
A.1.2 - Innovation and Modernization	Clearing Fund	\$734,570

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

No other programs provide the same services that DIR provides through the Technology Guidance and Innovation function. Texas' information resources are decentralized, with every agency operating its own technology department. As the Legislature recognized in DIR's enabling statute, there is a need for DIR to lead in technology management and resource planning to maximize efficiency, set standards, and provide guidance. Many agencies have limited technology resources and turn to DIR for guidance and collaborative opportunities.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

DIR works with other customer organizations to assist in creating and implementing innovative strategies and solutions.

The Statewide Project Delivery Program coordinates and collaborates with all Texas state agencies and institutions of higher education to determine best practices for supporting compliance with statutory requirements regarding IT project management. DIR serves as the authority on IT project management for the State of Texas.

DIR gains insight into potential areas of duplication through the IRM discussion list, questions on the IT leadership survey conducted as part of the statewide IT strategic planning process, and the Information Resources Deployment Review (IRDR).

The Statewide Digital Accessibility Program provides website scanning to state agencies and institutions of higher education. State agencies and institutions of higher education choosing to participate in the program must complete a current memorandum of understanding. Once

DIR approves the memorandum of understanding, the requesting state agency or institution of higher education website will be set up for scanning with the designated users added.

DIR also collaborated with other state agencies, institutions of higher education, and the private sector on the Texas Workgroup for Blockchain Matters in 2021 and 2022. The Work Group comprised 16 appointed members including a representative from DIR appointed by the Governor. The group developed a master plan for the expansion of the blockchain industry in Texas and recommended policies and state investments in connection with blockchain technology.

The Work Group began meeting monthly in December 2021 and studied seven areas including Commercial Law and Contracts, Digital Identity, Decentralized Autonomous Organizations, Energy, Finance, Government Use Cases and Official Record keeping systems.

Throughout 2022, the seven subcommittees researched the current state of blockchain in Texas and held two public hearings. DIR participated in the government subcommittee, which was tasked with identifying government use cases for blockchain.

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

DIR coordinates with other state agencies and institutions of higher education through the strategic planning process. The State Strategic Plan Advisory Committee is required to include at least nine—but not more than more than 21—members appointed by DIR’s Executive Director with approval from the Board of Directors.³³⁶

Figure 94 State Strategic Plan Committee Requirements

Representation	Minimum Required
State Agency	2
State University System or Institution of Higher Education	1
Public Representative	1
Local Government	1
Technology Industry	3
Federal Agency	1

k) If contracted expenditures are made through this program please provide:

A Short Summary of The General Purpose of Those Contracts Overall

This program manages contracts that provide event management services, accessibility website

³³⁶ [1 Tex. Admin. Code § 201.5.](#)

scanning, an accessibility program learning management system, and technology research services.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$351 thousand in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 11 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from March 2021 through August 2022 for these contracts. The funding source was revenue from the Cooperative Contracts program.

The Method Used to Procure Those Contracts

These contracts were procured competitively through request for quote and TXSmartbuy.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-TSO-4099/DIR-RFQ-12-FY21-ELT*	Gartner Group	Provides research and advisory services for ELT.	\$131,366.37
DIR-TSO-3840/DIR-CTS-LA-SA-0001	Level Access Inc.	Provides accessibility training for DIR, state agencies, and institutions of higher education.	\$49,500.00
DIR-TSO-4162/RFQ-37-FY21-SA-0009	Carahsoft Technology Corporation	Provides Google Dialogflow Chatbot Development services for CTO program.	\$49,341.76
DIR-TSO-3840	Level Access Inc.	Provides accessibility IT software and related services.	\$33,650.00
DIR-TSO-4128/DIR-RFQ-12-FY21-SA-0003*	IDC Research Inc.	Provides research and advisory services for ELT.	\$30,367.00

The Methods Used to Ensure Accountability for Funding and Performance

DIR's contract and vendor management processes ensure that contractors perform in accordance with all contractual requirements. Active management of service level agreements also ensures that vendors deliver in accordance with each contract.

A Short Description of Any Current Contracting Problems.

Not applicable.

I) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

Under the Technology Guidance and Innovation function, DIR produces some reports based on outdated statutory language for reporting requirements. These outdated requirements are noted in DIR's evaluation of reporting requirements in Exhibit 16.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

DIR's Artificial Intelligence Center of Excellence received the State IT Innovation of the Year Award as part of the 2021 StateScoop 50 Awards.

o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility).

DIR does not regulate technology compliance. However, state agencies self-report compliance with the following requirements related to reviewing information resources deployment, designating an Electronic and Information Resources Accessibility Coordinator, designating an Information Resources Manager, and identifying continuing education for Information Resources Managers.

Information Resources Deployment Review (IRDR)

Why the Regulation Is Needed

The Information Resources Manager at each Texas state agency and institution of higher education are required to conduct an Information Resources Deployment Review (IRDR) every two years. The IRDR is a biennial standardized survey mandated by [Government Code Section 2054.0965](#) that provides a review of the operational aspects of each agency's information resources deployment in support of the agency's mission, goals, and objectives.³³⁷

The data submitted through the IRDR confirms that the agency is in compliance with the state's information resources-related statutes, rules, and standards. The data submitted through the IRDR is used to measure an agency's progress against the technology goals established in the State Strategic Plan (SSP). DIR uses the information collected through the IRDR to improve the programs, services, and solutions available to state agencies and identify certain compliance issues that need resolution. The data is used to inform several reports to the Legislature and to advocate for technology policy changes as needed.

Institutions of higher education are required by [1 Texas Administrative Code Section 213.40](#) to

³³⁷ [Gov't Code § 2054.0965](#).

complete an Electronic and Information Resources (EIR) accessibility survey.³³⁸ The online submission of IRDR Sections 1.03, 2.02, and 2.03 through SPECTRIM satisfies this reporting requirement. Institutions of higher education are exempt from reporting additional IRDR results to DIR by [Education Code Section 51.406](#), but they do have the option to report all completed IRDR sections if desired.³³⁹ The EIR accessibility survey measures state agencies' EIR accessibility progress, gauges compliance with state accessibility requirements, and helps understand barriers to ensuring accessibility of state IT resources.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

[Government Code Section 2054.097](#) requires DIR to review responses to the IRDR to ensure state agency compliance with state technology standards and statutes and the State Strategic Plan.³⁴⁰

Follow-up Activities Conducted When Non-compliance Is Identified

A state agency found to be non-compliant in any question in Part 2 of the IRDR must submit an Information Resources Corrective Action Plan (IR-CAP) for that item. An IR-CAP is a detailed plan that outlines the steps and timeframe for an agency to achieve compliance with state information resources standards.

Actions Available to the Agency to Ensure Compliance

DIR is required to report to state leadership those agencies that fail to submit an approved plan for any items. IR-CAPs are reviewed pursuant to Texas Administrative Code (TAC) rules.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Designating an Electronic and Information Resources Accessibility Coordinator (EIRAC)

Why the Regulation Is Needed

State agencies and institutions of higher education are required to designate an EIR Accessibility Coordinator who shall be organizationally placed to facilitate institution-wide EIR accessibility compliance and practices in support of their internal accessibility policy.³⁴¹ State government is required to follow the [Americans with Disabilities Act Section 508](#) procurement practices and industry standards for web accessibility.³⁴² These requirements are carried over to State of Texas government code and administrative code. Compliance with these standards and regulations requires a significant amount of coordination with agency roles, staff training, policy setting, process improvement, and maintaining a knowledge base in digital accessibility

³³⁸ [1 Tex. Admin. Code § 213.40](#).

³³⁹ [Educ. Code § 51.406](#).

³⁴⁰ [Gov't Code § 2054.097](#).

³⁴¹ [1 Tex. Admin. Code §§ 213.21, 213.41](#).

³⁴² [29 U.S.C. § 794\(d\)](#).

that supports the agency. Assigning these tasks to one point of contact in the agency fosters consistency in executing policies, processes, and outreach within the agency to support compliance. DIR is charged with the same functions (but at a statewide level) and provides support to all agencies supporting their compliance requirements. The Digital Accessibility program supports 176 state agencies; therefore, having a single point of contact at each agency is more efficient for DIR to fulfill its obligations with governing statute and rules.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

Agency eligibility for the services and programs under the Digital Accessibility program is determined by the Program Administrator. DIR does not perform accessibility inspections or audits, nor does the State Auditor. A selection of the primary processes within the program include:

- Reviewing and approving EIRAC designations;
- Setting up Access Academy accounts for employees;
- Setting up web scanning accounts for agencies;
- Developing outreach events and resources;
- Participating in community engagement; and
- Working with program vendors to ensure completion of support tickets, timely contract renewals, and excellent customer experiences.

Follow-up Activities Conducted When Non-compliance Is Identified

The Statewide Accessibility Program Administrator will work with the agency's Information Resources Manager or Chief Information Officer (CIO) to ensure that an EIRAC is designated. Working with the CIO or Information Resources Manager includes making email communications and phone calls as needed. DIR provides resources and information to support the agency in other areas of non-compliance, such as procurement exceptions, website scanning, agency policy, and vendor non-compliance with procurement requirements.

Actions Available to the Agency to Ensure Compliance

DIR does not have processes in place to ensure that agencies are compliant with [Government Code Chapter 2054 Subchapter M](#),³⁴³ [1 Texas Administrative Code 206](#),³⁴⁴ and [1 Texas Administrative Code Chapter 213](#)³⁴⁵ except for Sections 213.21 and 213.41. DIR tracks the agencies' EIRAC designees and performs a periodic review to ensure that the current designee is active (and that inactive designees are replaced). DIR provides resources to support agency compliance with the Texas Administrative Code by providing a digital accessibility learning management system and automated website scanning. DIR does not monitor agency activity or web scanning results. Government Code and Texas Administrative Code put the onus of compliance on the agencies. DIR is responsible only for providing the rules and supporting the

³⁴³ Gov't Code Chapter 2054, Subchapter M.

³⁴⁴ 1 Tex. Admin. Code Chapter 206.

³⁴⁵ 1 Tex. Admin. Code Chapter 213.

agencies.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Designating an Information Resources Manager (IRM)

Why the Regulation Is Needed

Each state agency and institution of higher education is required to designate an employee of the agency to serve as the agency's IRM.³⁴⁶ IRMs are the primary point of contact for an agency with DIR. DIR communicates announcements, IT policy changes, and IT reporting requirements for the agency to the IRMs.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

Before an IRM designation is accepted by DIR, DIR reviews the designation to determine that the IRM meets all eligibility requirements. IRM designations must be approved by the designating agency's head (Executive Director or equivalent position) or Deputy Executive Director. Agencies submit a designation letter and a copy of the agency's organizational chart to confirm that that an IRM reports to the Executive Director or equivalent position. DIR confirms the agency's biennial information resources budget to determine the appropriate agency level, which determines the number of continuing education hours the IRM is required to submit.

Follow-up Activities Conducted When Non-compliance Is Identified

DIR communicates to agencies that have not identified an IRM that they are required to designate one. If an IRM does not meet eligibility requirements, DIR will not accept the designation. If an agency fails to designate an IRM, the IRM designation will default to the agency's Executive Director.

Actions Available to the Agency to Ensure Compliance

DIR may reach out to an agency that remains out of compliance with an official letter to the agency's Executive Director.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Identifying Continuing Education for IRMs

Why the Regulation Is Needed

DIR is required to provide mandatory guidelines to state agencies regarding continuing

³⁴⁶ [Gov't Code § 2054.071](#).

education requirements needed for IRMs and require IRMs to report their compliance with the requirements to DIR.³⁴⁷ IRMs oversee the acquisition and use of valuable information technology within agencies. Continuing education helps IRMs ensure that all information resources are acquired, managed effectively, and in compliance with regulations and agency policies.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

DIR communicates the requirements of the IRM role to newly designated IRMs and regularly hosts IRM orientations. The number of continuing education hours required for an IRM is determined by the size of their agency's biennial information resources budget. Hours for IRMs designated mid-year are prorated based on the month of their designation. IRMs report continuing education hours to DIR annually. DIR reviews the continuing education hours submitted by IRMs to determine compliance following the annual deadline of August 31 of each year.

Follow-up Activities Conducted When Non-compliance Is Identified

DIR works with IRMs to help facilitate compliance. Continuing education requirements and instructions for reporting continuing education hours are communicated to IRMs by email during IRM orientations and at IRM Continuing Professional Education informational sessions held prior to the August 31 deadline for submitting hours. DIR will meet one on one with IRMs to assist with completing requirements. Prior to the annual deadline, DIR will reach out to IRMs to ensure that they are aware of continuing education requirements.

Actions Available to the Agency to Ensure Compliance

The IRM Outreach and Education Coordinator sends an agency memorandum that lists agencies found non-compliant to DIR leadership following the annual continuing education deadline. The memorandum includes recommendations for any necessary actions from DIR executive management. DIR may reach out to an agency that remains out of compliance with an official letter to the agency's Executive Director.

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

Submitting Project Delivery Framework Documents to the Quality Assurance Team (QAT)

Why the Regulation Is Needed

DIR is a member of the QAT that develops and recommends policies and procedures to improve the development, implementation, and return on investment for state agency information resources technology projects.³⁴⁸ Consistent project management helps agencies

³⁴⁷ [Gov't Code § 2054.076.](#)

³⁴⁸ [Gov't Code § 2054.158.](#)

successfully deliver projects on budget and on schedule, providing value to taxpayers and stakeholders. To make project management easier, DIR has collaborated with many statewide agencies to create the Project Delivery Framework templates for major information resources projects, or projects that are \$5 million or more. The Project Delivery Framework is a set of templates that provide a review of the scope, costs, schedule, and outcomes of each agency's major information resources projects in support of the agency's mission, goals, and objectives.³⁴⁹

The data submitted through the Framework confirms that the agency is in compliance with the state's information resources related statutes, rules, and standards. The data submitted through the Framework is also used to measure an agency's progress against the technology goals established in the State Strategic Plan. DIR uses the information collected through the Framework to help improve the programs, services, and solutions available to state agencies and identify certain compliance issues that need resolution. The QAT also uses the data to inform several reports to the Legislature and to educate on the state of technology projects and recommended policy changes.

The Scope of—and Procedures for—Inspections or Audits of Regulated Entities

The policies for this requirement are set forth in the QAT [policies and procedures](#) guide.

Follow-up Activities Conducted When Non-compliance Is Identified

A state agency found to be non-compliant is subject to all corrective actions listed in the QAT [policies and procedures](#), including, but not limited to, at the QAT's discretion:

- Require independent verification and validation services for high-risk projects;
- Request formal review by the State Auditor's Office;
- Hold regular status meetings with executive staff to provide analysis and plans for resolving major issues;
- Issue a formal corrective action plan and report to agency and state leadership; and
- Recommend the cancellation of the project or contract and report to agency and state leadership for poorly managed projects or excessive cost overruns.

Actions Available to the Agency to Ensure Compliance

DIR is required to participate in the QAT, providing guidance to the team for technology and project management issues. The entire QAT votes on and approves all actions taken by DIR. The QAT reports to state leadership those agencies that fail to submit Framework documents for any major information resources projects. QAT prepares an annual report on all statewide activity, compliance, trends, lessons learned, and recommendations for major information resources projects in the state. The report is designed to help agencies avoid common project pitfalls that lead to missed deadlines or budget overruns.

³⁴⁹ [Gov't Code Chapter 2054, Subchapter J.](#)

Procedures for Handling Consumer and Public Complaints against Regulated Entities

Not applicable.

p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VII. Guide to Agency Programs – Texas.gov



The mission of the Texas Department of Information Resources (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and **offering innovative and cost-effective solutions for all levels of government.**

a) Provide the following information at the beginning of each program description.

Name of Program or Function: Texas.gov

Location/Division: William P. Clements Bldg., 300 West 15th Street, Austin, TX 78701

Contact Name: Dale Richardson, Chief Operating Officer

Statutory Citation for Program:

[Government Code Chapter 2054, Subchapter I, Statewide Technology Centers](#)

[Government Code Chapter 2054 Subchapter K, System for Occupations Licensing Transactions](#)

[Government Code Chapter 2054, Subchapter O, Major Outsourced Contracts](#)

[Government Code Chapter 2055, Electronic Grant System](#)

b) What is the objective of this program or function? Describe the major activities performed under this program.



The objective of Texas.gov is to enable Texas state agencies and eligible local governments and the constituents they serve to cost-effectively conduct government business online.

Texas.gov is the state's official website and a trusted resource for Texans to access government information and complete government business in an easy, secure, and user-friendly way. Texas government entities have access to secure, payment card industry compliant products, which allow for online and over-the-counter payments with credit and debit cards and Automated Clearing House (ACH) checks. Texas.gov provides services to over 300 state and local customers, processing Texan requests for items such as license renewals, vehicle registrations, and vital records.

Over the last 20 years, the program has evolved from an online portal designed to be accessed from a desktop or laptop computer to a mobile-friendly, integrated website that allows Texans to take care of government business anywhere, from any kind of device, and without having to stand in line at a government office.

The Texas.gov function enables state agencies, local governments, and institutions of higher education to provide simple, accessible, and secure online digital government services to Texans. Through the Texas.gov program, customer organizations can access digital transformation solutions that include:

- Secure, cloud-based, and compliant payment processing services;
- Application development, web design services, constituent marketing, tools to gauge customer satisfaction, and operations support;
- Infrastructure hosting services, including cloud services, through DIR's Shared Technology Services (STS); and
- A help desk for entities and people using the hosted services.

In 2022, Texas.gov processed nearly 58 million transactions, totaling approximately \$2.3 billion for Texas government entities.

Texas.gov provides Texans with government interactions that meet or exceed statutory requirements in addition to industry-standard best practices for accessibility, security, and privacy. The quality of interaction facilitated through the Texas.gov program is on par with that of commercial organizations. All financial transactions are integrated with the Texas Comptroller of Public Accounts financial systems.

In 2021, DIR launched Texas by Texas (TxT), the digital government assistant, as part of the Texas.gov program. TxT is a mobile-first digital government experience that offers an even easier, faster, and more secure way for Texans to take care of their government business than traditional Texas.gov payment processing. State agencies can integrate constituent-facing services, so Texans can complete services quickly and securely.

The vision for TxT is to serve as the one-stop shop for Texans for all government transactions. TxT is designed so that users no longer need to know or keep track of which agency is responsible for which program or service. TxT preemptively knows what services the user needs, when those transactions are due, and how to guide the user through any requisite processes. As more agencies onboard their services into TxT, more Texans will be connected to the secure ease of use and intuitive functionality of this reimagined vision for the delivery of government services. For example, when a user's vehicle registration requires renewal from the Texas Department of Motor Vehicles, TxT sends the user messages and alerts them that their car needs an inspection, and their registration sticker needs renewing. TxT shows the user the closest inspection stations, presents their renewal information to them, and allows them to track the status of their registration sticker. TxT can also alert users when their driver's license is due for renewal from the Texas Department of Public Safety, messaging users and guiding them through the renewal process.

As more agencies add their programs to TxT, additional services will be consolidated for Texans, eliminating the need for Texans to navigate and understand complex government structures to receive the services they require. TxT currently includes services from the Texas Department of Motor Vehicles, Texas Department of Public Safety, and one program at the Texas Department of Licensing and Regulations with the remaining programs planned once their new licensing platform is completed.

c) What information can you provide that shows the effectiveness and efficiency of this program or function?

Efficiency of Online and Mobile Transactions

While Texas.gov provides state agencies the opportunity to digitally transform their constituent-facing services, Texans and the state save both time and money by transacting through Texas.gov. According to a recent study,³⁵⁰ government transactions conducted face-to-face, by telephone, or through the mail cost exponentially more than online transactions. In addition, constituents save time and money by transacting with their government online because there is no line or phone queue to wait in for service. Additionally, constituents do not need to pay for transportation or travel costs to the government office or postage to mail a check. Texas.gov's online digital processing is estimated to save customer entities approximately \$18 million annually in in-person visits and mailing costs.

Efficiencies of DIR's TxT Native Mobile Application

TxT allows Texans to create a single user account for all state business. TxT also includes security steps to verify a user's identity and multi-factor authentication (MFA) to help keep accounts safe. Users can link and manage government-issued licenses and registrations, such as their driver's license and vehicle registration. Users can then access a personalized dashboard and to-do list to keep track of upcoming deadlines, securely store payment information, review transaction history, update notification preferences, and more. TxT sends proactive emails and text reminders (if opted into) when it's time for a user to act.

A single native mobile application for Texas state business provides significant cost-saving benefits to the state. DIR funds the ongoing maintenance and operations of TxT. State agencies are saved from the time and expense of building a native mobile application, which can be costly due to the development and maintenance costs incurred to comply with the requirements of the primary phone app stores, Google Play and the App Store.

TxT eliminates the advertising and marketing costs agencies would incur to their application. To advertise TxT, DIR and Deloitte drive Texans to Texas.gov and TxT through advertising and marketing campaigns supported by Deloitte, pursuant to the awarded contract for Texas.gov

³⁵⁰ [Deloitte Access Economics](#).

Services.

Texans also reap the benefits of Texas having only a single mobile application for state agencies. If each state agency had their own mobile application, Texans would need to keep track of each state agency's unique mobile application and remember which agency's mobile app is for what transaction type. This confusion would create an overwhelming obstacle to Texas' adoption of each mobile application. With TxT branded as the one mobile application for all Texas state government, user adoption is more efficient and cost effective for all.

Customer Satisfaction

Constituent Surveys

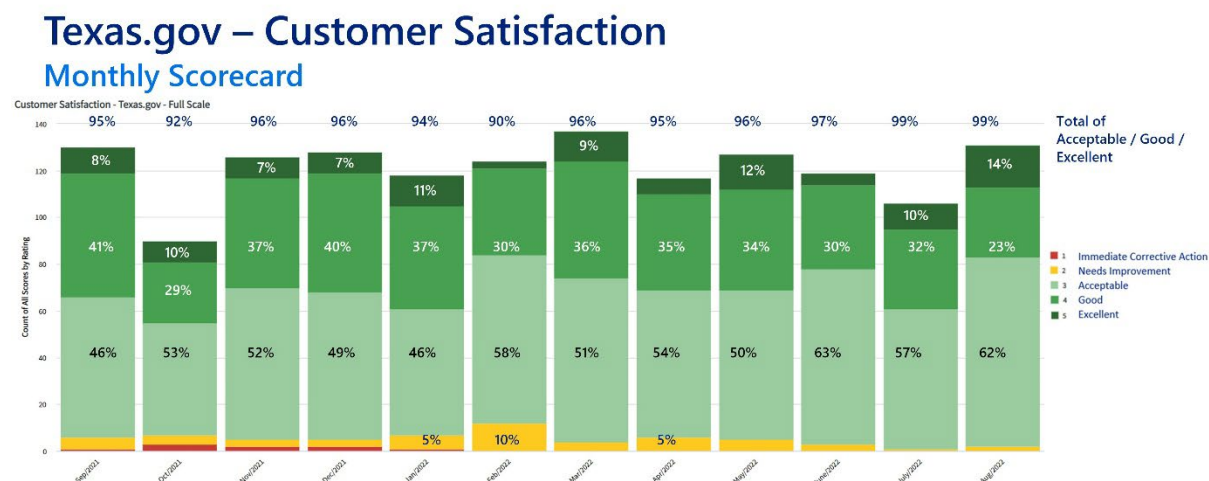
As the most publicly facing program of DIR, a key element of the Texas.gov program is measuring and evaluating constituent satisfaction with Texas.gov online services. From June 2020 to May 2022, over 70,000 respondents completed a voluntary survey upon completion of a Texas.gov online transaction. The results showed that:

- Eighty-eight percent (88%) Strongly Agreed or Agreed to the survey question "I would recommend this online service to someone else."
- Eighty-six percent (86%) Strongly Agreed or Agreed to the survey question "Overall I am satisfied with my experience."

Monthly STS Customer Scorecards

As a program of STS, public entity customers provide satisfaction ratings on Texas.gov service providers. The chart below reflects the overall customer satisfaction with the Texas.gov program for FY22.

Figure 95 Texas.gov Customer Satisfaction Monthly Scorecard



Vendor Performance Ratings

Vendor Service Level Agreements

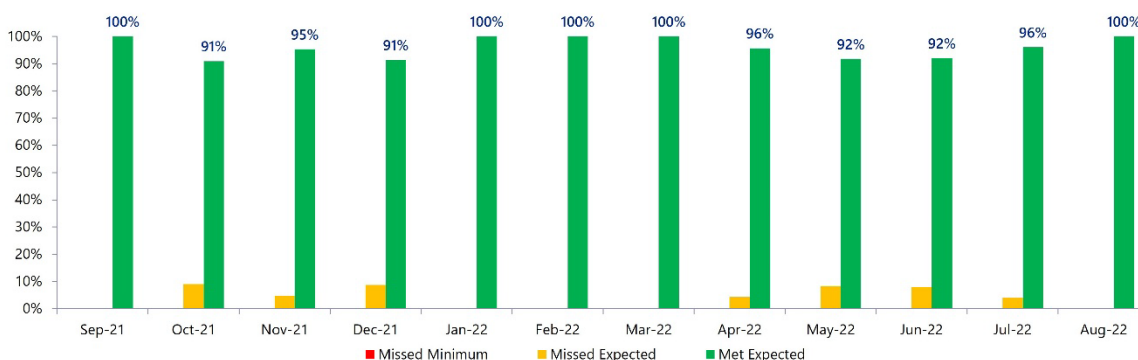
DIR tracks compliance with service metrics agreed upon between DIR and service providers

across the STS programs, including Texas.gov. Service level agreement performances are published to STS government entity customer dashboards each month.

Figure 96 Texas.gov Performance Management Service Level Agreements

Texas.gov – Performance Management

Service Level Agreements (SLAs)



d) Describe any important history regarding this program not included in the general agency history section, including how the services or functions have changed from the original intent. If the response to Section III of this report is sufficient, please leave this section blank.

2001

In 2001, the Texas Legislature tasked DIR with implementing “a state electronic Internet portal project” and establishing a common electronic infrastructure for state agencies and local governments.³⁵¹ This project, which would eventually become Texas.gov, is the state’s official website and digital government program that has served as a resource for Texans to access government information and services for almost two decades.

In 2003, two years after the creation of TexasOnline, the 78th Legislature amended statute with the express intention to allow greater access to the services provided through the portal by:

- Expanding the use of e-Pay, the online payment processing system, to allow state agency use of the service for over-the-counter transactions;
- Requiring state agencies to include a link to TexasOnline from their websites;
- Requiring additional state agencies to use the Common Occupational Licensing project; and
- Requiring DIR to create a web portal for veterans.

³⁵¹ [Gov’t Code §§ 2054.251-2054.274.](#)

2009

In 2009, DIR rebranded the TexasOnline portal as Texas.gov and entered a new contract for the management of Texas.gov, effective January 2010. In 2011, the Legislature amended statutory references from “TexasOnline” to the “state electronic Internet portal” to ensure the longevity of statutory references made to the official website for the State of Texas.

In September 2018, the Texas.gov program transitioned from a public-private partnership to a program that is funded and managed by the state. Control of the revenue, expenses, and services became the state’s sole responsibility, and the Legislative Budget Board appropriated to DIR an operations budget out of the transaction fee revenue. DIR awarded two contracts under the Texas.gov procurement. Under these contracts, two separate vendors would provide the services necessary to support Texas.gov with Deloitte providing Texas.gov application development services and Texas NIC, now called Tyler Technologies, providing Texas.gov payment processing. Due to the growth and critical nature of the Texas.gov program, DIR added the Texas.gov program to DIR’s outsourced managed services provided through the Data Center Services (DCS) program.

2020

In 2020, DIR released the Texas.gov Digital Identity Solution through Texas.gov to certain state agencies. This portal provides enhanced MFA capabilities, ensuring the continued security of state information and networks.

2021

In 2021, the 87th Legislature affirmed its confidence in Texas.gov as the state’s website when it passed legislation that prohibited another state agency from contracting with a third party for internet application development that duplicates a function of TxT. Exceptions could be made if the state agency notifies DIR of its intent to bid for the services, and DIR authorizes the agency to duplicate the function because the agency complied with certain other statutory requirements.

In 2021, DIR launched a major redesign of the [Texas.gov website](#). The upgraded site improved user experience with a new, mobile-friendly, and easy-to-navigate interface, enabling Texans to access the information or government services they need quickly and securely, anytime, anywhere, and on any device. The Texas.gov redesign also provides secure, direct access to more than 800 official government services, including vehicle registration renewals, driver’s license renewals, vital records, professional and occupational licenses, and recreational and hunting licenses. DIR and the Texas Department of Public Safety announced the availability of driver’s license renewals and vehicle registration renewals through TxT.

2022

In January 2022, DIR announced the launch of TxT, a digital assistant that allows Texans to create an online account, manage their government-issued licenses and registrations, receive proactive reminders when it’s time to take action, and complete transactions quickly and

securely. As mentioned previously, since officially launching in early 2022, 5.7 million Texans have created accounts on TxT and more than 9.2 million transactions have been processed.

e) List any qualifications or eligibility requirements for persons or entities affected by this program, such as licensees, consumers, landowners, for example. Provide a statistical breakdown of persons or entities affected.

The website and mobile application provided through Texas.gov are available to any member of the public with internet access.

The Texas.gov program is available to the following entities who are eligible for the services DIR provides:³⁵²

- State agencies;
- Local governments;
- The Legislature or a legislative agency;
- The supreme court, the court of criminal appeals, or a court of appeals;
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;
- An independent organization certified under Utilities Code Section 39.151, for the Electric Reliability Council of Texas (ERCOT) power region;
- The Texas Permanent School Fund Corporation;
- Assistance organizations, as defined by Government Code Section 2175.001;
- Open-enrollment charter schools, as defined by Education Code Section 5.001;
- Private schools as defined by Education Code Section 5.001;
- A private or independent institution of higher education, as defined by Education Code Section 61.003;
- Public safety entities, as defined by 47 U.S.C. Section 1401;
- Volunteer fire departments, as defined by Tax Code Section 152.001; and
- Government entities of another state.

³⁵² Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

f) Describe how your program or function is administered, including a description of the processes involved in the program or function. Include flowcharts, timelines, or other illustrations as necessary to describe agency policies and procedures. Indicate how field/regional services are used, if applicable.

Texas.gov Program Administration

The Texas.gov function is administered as an STS program by the Chief Operations Office. In addition to the duties described in that section, the following teams have duties specific to Texas.gov:

- The Vendor Management Office is responsible for managing the vendor relationship between DIR and the contracted Texas.gov vendors.
- The STS Project Engineering team is responsible for providing enterprise oversight and management of Texas.gov portfolios, programs, and projects.
- The STS Operations team is responsible for managing the Texas.gov vendors' delivery of services.
- The STS Customer Service team is responsible for managing DIR's relationship with Texas.gov customers.
- The STS Finance team is responsible for managing Texas.gov Legislative Appropriations Request Forecasting and Legislative Budget Board Reporting, Texas.gov invoicing, aged account receivables, and Texas.gov fee setting and validation.³⁵³
- The STS Contract Management team is responsible for monitoring and managing contracts between DIR and Texas.gov vendors.

The Texas.gov function is administered through vendor contracts for Texas.gov services, Texas.gov payment services, Multi-sourcing Services Integrator (MSI) services, Public Cloud Manager services, and Security Operations services.

DIR contracts with Deloitte to provide the following Texas.gov services:

- Managing Texas' statewide internet portal, the Texas.gov website;
- Developing and managing certain customer payment portal applications;
- Managing DIR's TxT native mobile application, which serves as a mobile digital assistant to Texans; and
- Developing marketing and advertising of Texas.gov and the TxT assistant to drive Texans to government business in a digital space rather than in-person service.

DIR contracts with Tyler Technologies (formerly Texas NIC) to provide the following Texas.gov payment services:

³⁵³ Gov't Code §§ [2054.0345](#), [2054.0346](#), [2054.380](#), [2059.151](#).

- Credit card and electronic check payment processing that is compliant with payment card industry requirements; and
- Integration with the Comptroller of Public Accounts' Unified Statewide Accounting System, so that Texas.gov accounting and treasury reconciliation is automated.

DIR contracts with Capgemini to provide the following Multi-sourcing Services Integrator (MSI) services:

- Texas.gov help desk, consisting of phone, email, and chat;
- Customer communication and relationship management;
- Payment card industry compliance documentation; and
- Integration and management of the Data Center Services (DCS) service component providers that support Texas.gov applications.

DIR contracts with Rackspace to provide the following Public Cloud Manager services:

- Infrastructure management and support of the public cloud compute hosting Texas.gov applications.

DIR contracts with Science Applications International Corporation (SAIC) to provide the following security operations services:

- Security monitoring and management; and
- Security policies and compliance oversight.

DIR manages the Texas.gov program and vendors through two governance models:

- DIR Operational Governance (DIR's internal operational management); and
- STS Owner-Operator Governance (DIR's external governance for customers and vendors).

DIR's Shared Technology Services Operational Governance Model

Texas.gov is administered under the operational governance model described in VII. Guide to Agency Programs – Shared Technology Services by the following DIR divisions and teams:

- Vendor Management Office;
- Project Engineering team;
- STS Operations team;
- STS Finance team;
- STS Contract Management team;
- Customer Engagement Office;
- Chief Procurement Office; and
- Office of the Chief Information Security Officer.

STS Owner-Operator Governance Model

DIR and DIR's customers have established an owner-operator governance model for STS programs, including Texas.gov. This owner-operator governance model is described in further detail in VII. Guide to Agency Programs – Shared Technology Services.

Texas.gov Program Processes

The processes for Texas.gov follow the processes established for DIR's Shared Technology Services function.

Texas.gov Program Exemptions

DIR administers state agency requests to be exempted from three statutory requirements regarding Texas.gov payment processing, the Texas.gov subscription framework, and the Texas.gov native mobile application. When Texas.gov exemption requests are received, the STS Governance Program Manager adds the request to the STS exemption log and routes the request to the Director of Vendor Management, Texas.gov Vendor Manager, and the Director of STS Finance. The request is then added as a topic to the next weekly Texas.gov Operational Governance Board (OGB) meeting for consideration. Once the OGB reaches a consensus, the STS Governance Manager routes the request for signatures.

Texas.gov Payment Processing Infrastructure

[Government Code Section 2054.113](#) prohibits a state agency from duplicating an infrastructure component or contracting with a third party for internet application development that duplicates a state electronic internet portal function without appropriate approval from DIR.³⁵⁴ This effectively requires a state agency to use the Texas.gov payment processor. DIR requires a customer to receive a Texas.gov Payment Processing Infrastructure exemption if the customer determines that they want to accept online payments outside of the services provided by the Texas.gov program.

To apply for exemption from the Texas.gov Payment Processing Infrastructure, agencies submit the following to DIR:

- A cover letter in the form of an executive summary;
- A completed Texas.gov Request for Infrastructure Exemption Agency Certification Form with required documentation attached, as published on the DIR website; and
- Financial details of the cost-benefit analysis.

The affirmations and documentation required by the form assure that the proposed native mobile application seeking exemption:

- Is in the financial best interest of the State of Texas;
- Protects constituents' sensitive personal information and any processed funds;
- Provides for use by people with a disability; and
- Integrates seamlessly with the Texas Comptroller of Public Account's Uniform Statewide Accounting System.

³⁵⁴ [Gov't Code § 2054.113](#).

Texas.gov Subscription Framework

[Government Code Section 2054.252\(e\)](#) requires DIR to charge a subscription fee for occupational licensing transactions to be paid by each licensing entity.³⁵⁵ DIR customers identified by [Government Code Section 2054.352](#) must submit a Texas.gov Subscription Framework exemption if they want to convert from the subscription fee model to a standardized convenience fee.³⁵⁶

To apply for exemption from the Texas.gov Subscription Framework, a state agency submits the following to DIR:

- A cover letter in the form of an executive summary, and
- A completed Texas.gov Request for Subscription Exemption Agency Certification Form, available on the DIR website, with required documentation attached.

The affirmations and documentation required by the form assure that the proposed non-subscription fee framework funding model:

- Is in the financial best interest of the State of Texas; and
- Incentivizes online constituent transactions over in person or mail transactions.

Texas.gov Native Mobile Application

[Government Code Section 2054.113\(c\)](#) requires DIR customers to obtain a Texas.gov Native Mobile Application exemption before contracting with a third party for internet application development that duplicates TxT functions.³⁵⁷

To apply for exemption from the Texas.gov Subscription Framework, a state agency must submit the following to DIR:

- A cover letter in the form of an executive summary;
- A completed Texas.gov Request for Subscription Exemption Agency Certification Form, available on the DIR website, with required documentation attached; and
- Financial details of the cost-benefit analysis.

The affirmations and documentation required by the form assure that the proposed native mobile application:

- Is in the financial best interests of the State of Texas;
- Protects constituents' sensitive personal information;
- Provides for use by people with a disability; and
- Integrates seamlessly with the Uniform Statewide Accounting System.

³⁵⁵ [Gov't Code § 2054.252\(e\)](#).

³⁵⁶ [Gov't Code § 2054.352](#).

³⁵⁷ [Gov't Code § 2054.113](#).

g) Identify all funding sources and amounts for the program or function, including federal grants and pass-through monies. Describe any funding formulas or funding conventions. Please specify state funding sources (e.g., general revenue, appropriations rider, budget strategy, fees/dues).

The majority of funding comes from transaction fees paid by constituents for completing transactions on Texas.gov as further discussed in Section V. Funding. Below is a chart explaining the types of Texas.gov fees.

Strategy	Method of Finance	Amount
B.3.1 - Texas.gov	Statewide Network Applications Account	\$40,656,031

Figure 97 Types of Texas.gov Fees

Fee Type	Description
Transaction Fee	Transactions fees are the most common Texas.gov fee structure and are a combination of a fixed fee per transaction (Texas.gov Fee) and a percentage of the transaction total (Texas.gov Percentage). The fee amount does not vary by credit card type and is not charged on Automated Clearing House (ACH) transactions. Customers determine whether Texas.gov fees are paid by the customer on behalf of the constituent or paid directly by the constituent.
Convenience Fee	Fixed fees per transaction, which usually apply to both credit cards and ACH. The fee varies by transaction type based on the scope of Texas.gov Application and Payment Processing services being provided. A convenience fee application may also be subject to a transaction fee.
Subscription Fee	Scaled fees based on the cost of the regulatory license purchase or renewal. Subscription fees are collected for license transactions processed through the Texas.gov portal (online) or other payment method (offline).

h) Identify any programs, internal or external to your agency, that provide identical or similar services or functions to the target population. Describe the similarities and differences.

Texas law allows DIR to provide a licensing system that can be used by any government entity responsible for regulatory licensing.³⁵⁸ As technology has advanced since this statute was drafted, there are numerous licensing platforms and technology vendors that specialize in various types of licensure applications, which are sold to—and used by—other states. Some of these platforms are more modern than the Texas.gov platform, and some are more limited in their capabilities in comparison to the Texas.gov customers' needs.

Texas.gov developed the TxT application that allows constituents to transact business with multiple agencies, all in one place. TxT further includes a native mobile application, which

³⁵⁸ [Gov't Code § 2054.252](#).

allows constituents to interact with these agencies from any kind of device: laptop, desktop, tablet, mobile phone, and more. As Texans increasingly prefer digital interactions with government, state agencies will increasingly need to find a way to authenticate constituents and provide applications effective on mobile devices. Under current law, state agencies are potentially able to procure applications that duplicate the functionality of TxT, which would degrade the value of TxT as Texas' single, consolidated point of contact for State of Texas business.

DIR developed Texas.gov, the state's official internet portal and consolidated payment processing system, which allows agencies to advertise their services on a single portal for all constituents to find. In addition, it allows the state to take advantage of volume-discounted payment processing fees for financial transactions.

i) Discuss how the program or function is coordinating its activities to avoid duplication or conflict with the other programs listed in Question H and with the agency's customers. If applicable, briefly discuss any memorandums of understanding (MOUs), interagency agreements, or interagency contracts.

[Government Code Section 2054.113](#) requires state agencies to notify DIR and obtain an exemption before contracting with a third party to build an internet application development that duplicates Texas.gov functions, including TxT native mobile application functions.³⁵⁹ This requirement ensures that Texans are able to have a single, secure, centralized, and mobile-friendly platform for interacting with government instead of having numerous native mobile applications with different functions and security protections. Texas.gov provides state agencies an already developed native mobile application to use instead of each agency building their own and duplicating existing technology, which results in greater cost to the state.

[Government Code Section 2054.113](#) also requires state agencies to notify DIR and obtain an exemption before duplicating the functionality of the Texas gov portal and payment processing.³⁶⁰

The benefits of using Texas.gov for mobile applications include:

- Cost savings to agency – native mobile applications are expensive to build based on the development and maintenance costs associated with the primary phone stores (Google Play and the App Store).
- Cost savings to the state - agencies can leverage an enterprise platform that is already built while DIR funds the ongoing maintenance and operations of the TxT product platform, including the native mobile application.

³⁵⁹ [Gov't Code § 2054.113](#).

³⁶⁰ *Id.*

- Providing Texans with a single, secure, centralized, and mobile-friendly platform for interacting with government, instead of having numerous native mobile applications with different functions and security protections.
- Increased security and protection of access to constituent data, and the assurance that the state is transacting business with a verified constituent which also leads to decreased fraud.
- Quicker speed to market for the agency because the platform is already built.
- Increased awareness of agency services through Texas.gov's marketing program (since the agency does not have to market a new standalone application to constituents).

j) If the program or function works with local, regional, or federal units of government, include a brief description of these entities and their relationship to the agency.

The following local and regional entities are eligible for the services DIR provides, including programs within the Texas.gov function:³⁶¹

- Local governments, including counties, municipalities, school districts, and junior college districts;³⁶²
- Out-of-state government entities;
- Volunteer fire departments;
- Public safety entities; and
- Public hospitals owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority.³⁶³

These entities sign an interlocal contract agreement with DIR to receive STS, including Texas.gov.

k) If contracted expenditures are made through this program please provide:

A Short Summary of The General Purpose of Those Contracts Overall

This program primarily utilizes contracts to operate the Texas.gov website including application

³⁶¹ Effective September 1, 2023, these entities are eligible for DIR programs if the DIR Executive Director determines that participation is in the best interest of the state. Before the passage of House Bill 4553 by the 88th Legislature, Regular Session, all entities except open-enrollment charter schools were eligible for various DIR programs, but statutory eligibility was not uniform with different eligibility requirements for different programs.

³⁶² [Gov't Code § 2054.003\(9\)](#).

³⁶³ [Gov't Code § 2157.068\(j\)](#); *see also* [Act of September 1, 2023, 88th Leg., R.S., ch. 242 \(H.B. 4553\), § 1 \(to be codified at Gov't Code § 2054.0525\)](#).

development and maintenance services, and payment processing services.

The Amount of Those Expenditures in Fiscal Year 2022

During FY22, this program spent approximately \$38.3 million in contracted expenditures.

The Number of Contracts Accounting for Those Expenditures

In FY22, there were 29 contracts accounting for these expenditures.

The Award Dates and Funding Source for Those Contracts

The award dates range from October 2017 through August 2022 for these contracts. The funding source for these contracts is revenue generated through transactions completed on the Texas.gov portal and payments received from governmental entities for specific application development projects completed by the Texas.gov program.

The Method Used to Procure Those Contracts

These contracts were procured through request for offer and request for quote.

Top Five Contracts by Dollar Amount, Including Contractor and Purpose

Contract Number	Vendor Name	Purpose	FY22 Expended
DIR-ESS-TGOV-SVCS-254	Deloitte Consulting Inc.	Provides application development and maintenance services for Texas.gov.	\$30,080,927.26
DIR-ESS-MSI-407	Capgemini America Inc.	Provides multi-sourcing services integration for Texas.gov.	\$4,254,016.44
DIR-PCM-MSA-436	Rackspace US, Inc.	Provides public cloud infrastructure for Texas.gov.	\$2,889,282.69
DIR-TPC-MSA-432	Atos Governmental IT Outsourcing Services, LLC	Provides private cloud infrastructure for Texas.gov.	\$434,462.34
DIR-ESS-ODP-428	Tyler Technologies, Inc. (Socrata)	Provides open data and closed data portal services through Texas.gov.	\$252,525.00

The Methods Used to Ensure Accountability for Funding and Performance

DIR's contract and vendor management processes ensure that contractors perform in accordance with all contractual requirements. Active management of service level agreements also ensures that vendors deliver in accordance with each contract.

A Short Description of Any Current Contracting Problems

Not applicable.

l) Provide information on any grants awarded by the program.

Not applicable.

m) Are there any barriers or challenges that impede the program's performance, including any outdated or ineffective state laws? Explain.

A hinderance for the Texas.gov program is that while online transactions are the most cost-effective method for state government to interact with constituents, state agencies are not incentivized to move more services online. Even though options like mail and in-person visits cost the state more in operation and staffing costs, Texans do not have to pay an extra processing fee for those transactions, like they do for most transactions on Texas.gov.

If Texans could do all—or at least the majority of—government business online, the potential budget savings could be significant due to the shared infrastructure afforded through the Texas.gov program. To determine an estimate of the savings, an analysis is needed comparing how much agencies are spending on processes that are not online versus the potential reduction of costs agencies may achieve were they to transition to Texas.gov.

To truly achieve digital transformation and reduce state costs overall, agencies need to be incentivized to reduce their expensive in-person processes. If the state shifted its investment away from expensive processes to integrate more types of agency services on Texas.gov and TxT, both state leadership and the public that use these services would benefit. Shifting more processes to Texas.gov and TxT would:

- Streamline the legislative appropriation requests into a centralized portal instead of receiving multiple requests from agencies. The Texas.gov program would be accountable for outcomes and providing legislative leadership increased visibility, transparency, and control.
- Provide the public with one location for multiple government services thus offering a more modern and customer-centric government experience for Texans.
- Save state funds through shared infrastructure and applications.

n) Provide any additional information needed to gain a preliminary understanding of the program or function.

A preliminary understanding of the Texas.gov function can be gained through the following supplementary resources:

- [Texas by Texas video](#);
- [Texas.gov website](#); and
- [TxT website](#).

- o) Regulatory programs relate to the licensing, registration, certification, or permitting of a person, business, piece of equipment, or other entity (e.g., a facility).

Not applicable. Texas.gov does serve, however, as a portal for hundreds of government services for Texans and businesses, including driver services, professional and occupational licensing, vital records, business resources, online payments, and more.

- p) For each regulatory program, if applicable, provide detailed information on complaint and regulatory actions, including investigations and complaint resolutions.

Not applicable.

VIII. Statutory Authority and Recent Legislation

- a) Fill in the following charts, listing citations for all state and federal statutes that grant authority to or otherwise significantly impact your agency. Do not include general state statutes that apply to all agencies, such as the Public Information Act, the Open Meetings Act, or the Administrative Procedure Act. Provide information on Attorney General opinions from fiscal years 2015-20, or earlier significant Attorney General opinions, that affect your agency's operations.

Texas Department of Information Resources

Statutes

Exhibit 13: Statutes/Attorney General Opinions

Citation/Title	Authority/Impact on Agency (e.g., "provided authority to license and regulate nursing home administrators)
Government Code Chapter 2054	Enabling statute for the Texas Department of Information Resources
Government Code Chapter 2054, Subchapter D	Information Resources Managers
Government Code Chapter 2054, Subchapter E	State Strategic Plan for Information Resources Management
Government Code Chapter 2054, Subchapter F	Oversight of Major Information Resources Projects, Information Technology Council for Higher Education, Posting of High Value Datasets, Information Security Plan, Designated Information Security Officer, Designated Data Management Officer
Government Code Chapter 2054, Subchapter G	Project Management Practices

Citation/Title	Authority/Impact on Agency (e.g., "provided authority to license and regulate nursing home administrators)
Government Code Chapter 2054, Subchapter H	Telecommunications Planning
Government Code Chapter 2054, Subchapter I	State Electronic Internet Portal (Texas.gov)
Government Code Chapter 2054, Subchapter J	Texas Project Delivery Framework
Government Code Chapter 2054, Subchapter K	Electronic System for Occupational Licensing Transactions
Government Code Chapter 2054, Subchapter L	Statewide Technology Centers (Shared Technology Services)
Government Code Chapter 2054, Subchapter M	Electronic and Information Resources Accessibility
Government Code Chapter 2054, Subchapter N-1	Cybersecurity
Government Code Chapter 2054, Subchapter N-2	Volunteer Incident Response Team
Government Code Chapter 2054, Subchapter O	Major Outsourced Contracts
Government Code Chapter 2054, Subchapter Q	Legacy System Modernization
Government Code Chapter 2059	Network Security
Government Code Chapter 2059, Subchapter C	Network Security Center
Government Code Chapter 2059, Subchapter E	Regional Network Security Centers
Government Code Section 2155.007	Procurement Coordination Committee
Government Code Chapter 2155, Subchapter I	Multiple Award Contracts
Government Code Chapter 2157	Information Technology Cooperative Contracts
Government Code Chapter 2170	Telecommunications Services
Government Code Section 403.027	Digital Signatures
Government Code Section 406.104	Online Notarization
Government Code Sections 411.0765, 411.1404, and 411.1405	Limited Disclosure of Criminal History Information
Government Code Section 418.0195	Disconnection of State Network Due to External Threat
Government Code Chapter 421	Homeland Security Council
Government Code Chapter 434, Subchapter C	Veterans Website
Government Code Section 441.010	Searchable Central Grant Database
Government Code Section 441.182	Records Management Training
Government Code Section 441.203	Records Management Interagency Coordinating Council

Citation/Title	Authority/Impact on Agency (e.g., "provided authority to license and regulate nursing home administrators)
Government Code Section 531.013	Electronic Availability of Human Services Providers Technical Assistance
Government Code Section 531.024	Health and Human Services Data Sharing
Government Code Section 531.0313	Texas Health Information and Referral Network
Government Code Section 531.0317	Website of Programs and Services Offered by Health and Human Services Agencies throughout State
Government Code Section 535.051	Liaison for Faith- and Community-Based Organizations
Government Code Section 551.127	Minimum Standards Videoconference at Open Meetings
Government Code Section 552.009	Open Records Steering Committee for Electronic Availability of Public Information
Government Code Section 656.050, 656.052	Training for Contracting and Purchasing Information Resources Technologies
Government Code Chapter 2060	Interagency Data Transparency Commission
Government Code Section 2101.040	Enterprise Resource Planning Advisory Council
Government Code Section 2151.004	General Services Commission Transfer
Government Code Section 2261.258	Additional Monitoring of Major Information Resources Projects
Government Code Section 2262.051	Contract Management Guide
Government Code Chapter 2262, Subchapter C	Contract Advisory Team
Business and Commerce Code Chapter 304, Subchapter B	Texas No-Call List
Business and Commerce Code Chapter 322	Uniform Electronic Transactions Act
Code of Criminal Procedure Article 66.351	Criminal Justice Information System Biennial Plan
Code of Criminal Procedure Article 66.401	Criminal Justice Program Grants
Health and Safety Code Section 105.003	Texas Statewide Health Coordinating Council
Health and Safety Code Section 361.965	Computer Equipment Recycling Program
Health and Safety Code Chapter 771	Commission on State Emergency Communications
Local Government Code Section 195.008	Electronic Recording Advisory Committee
Occupations Code Section 1701.654	Body Worn Camera Services
Transportation Code Section 502.357	Motor Vehicle Registration Financial Responsibility Fee

Citation/Title	Authority/Impact on Agency (e.g., "provided authority to license and regulate nursing home administrators")
Transportation Code Chapter 601, Subchapter N	Motor Vehicle Financial Responsibility Verification Program
Utilities Code Chapter 31, Subchapter B	Cybersecurity Coordination Program for Utilities

Attorney General Opinions

Attorney General Opinion No.	Impact on Agency
N/A	

b) Provide a summary of significant legislation regarding your agency by filling in the charts below or attaching information already available in an agency-developed format. Briefly summarize the key provisions. For bills that did not pass but were significant, briefly explain the key provisions and issues that resulted in failure of the bill to pass (e.g., opposition to a new fee, or high cost of implementation). Place an asterisk next to bills that could have a major impact on the agency.

Texas Department of Information Resources

Exhibit 14: 88th Legislative Session

Legislation Enacted

Bill Number	Author	Summary of Key Provisions
SB 271	Johnson Shaheen	- Relating to state agency and local government security incident procedures. - Requires local governments to report cybersecurity incidents to DIR. - Effective September 1, 2023.
SB 621	Parker Capriglione	- Relating to the position of Chief Information Security Officer in the Department of Information Resources. - Establishes the Chief Information Security Officer to oversee cybersecurity matters in the state. - Effective September 1, 2023.
SB 1893	Birdwell	- Relating to prohibiting the use of certain social media applications and services on devices owned or leased by government entities. - Requires DIR and the Department of Public Safety (DPS) to jointly develop a model policy on prohibiting covered applications for government entities to use in developing their own policies. - Requires DIR and DPS to identify social media applications that pose a risk to the state. Requires DIR to annually publish on its website a list of applications that pose a risk to the state. - Effective immediately.

Bill Number	Author	Summary of Key Provisions
HB 584	Capriglione	· Relating to the development of a state information technology credential offered by a public junior college or public technical institute to address shortages in the state information resources workforce. · Authorizes DIR to partner with a public junior college district or public technical institution to offer a program leading to a state information technology credential to address shortages in the state information resources workforce. · Effective September 1, 2023.
HB 2060	Capriglione	· Relating to the creation of the artificial intelligence advisory council. · Establishes the Artificial Intelligence Advisory Council, which includes DIR's Executive Director or designee, and requires DIR to provide administrative support for the council. · Effective immediately.
HB 3730	Wilson	· Relating to the directory of users of the centralized telephone service for entities in the Capitol Complex. · Adds email addresses to the centralized telephone service and email addresses directory that DIR is required to prepare annually. Requires state agencies to provide DIR email addresses for inclusion in the directory. · Effective September 1, 2023.
HB 4553	Longoria	· Relating to the eligibility of certain entities for services and commodity items provided by DIR and the statewide technology centers. · Establishes a consistent list of entities eligible for DIR services, subject to DIR's Executive Director determining that a particular entity's participation in the service is in the state's best interest. · Specifies that DIR can provide technology services through the statewide technology centers, other than telecommunications services governed by Government Code Chapter 2170. Removes DPS' exception from participation in the statewide technology centers. · Allows DIR to provide services through the statewide technology centers to an eligible entity. · Allows DIR to provide products and services requested by a single eligible entity through the Cooperative Contracts program. · Effective September 1, 2023.

Legislation Not Passed

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
SB 498	Johnson	· Relating to the operation of statewide technology centers. · Would have authorized DIR to provide services to a single government entity through the statewide technology centers, rather than requiring two or more entities. (Included in HB 4553.) · Would have DIR specify through rule the services that a statewide technology center is authorized to provide. · Vetoed by the Governor for conflicting with HB 4553.
SB 782 HB 984	Birdwell Capriglione	· Relating to the employment of a Chief Privacy Officer at DIR.

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
		· Would have required DIR's Executive Director to employ a Chief Privacy Officer to assist state agencies with legal and policy matters involving data privacy. The Chief Privacy Officer would conduct a biennial review of the privacy practices of state agencies, develop best practices to ensure compliance with privacy laws, and provide guidance to state agencies. · SB 782 was referred to the Senate Committee on Business and Commerce but did not receive a hearing. HB 984 was removed from the House Local Calendar.
SB 717 HB 4944	Paxton Buckley	· Relating to public school cybersecurity controls, student data privacy protection, cybersecurity requirements, technical assistance, and cybersecurity risk assessments provided by DIR for public schools. · Would have required the Texas Education Agency (TEA) Commissioner to adopt security controls and requirements for K-12, open-enrollment charter schools, and vendors of school districts through consultation with DIR. Would have authorized DIR to provide technical assistance to K-12 and open enrollment schools in implementing the security requirements through services offered by third parties, procuring technology for K-12, recommending to the Legislative Budget Board that K-12 schools migrate to the Angelo State Data Center, and/or using the Regional Security Operations Center services. Would have permitted DIR to adopt rules and perform risk assessments for K-12 at the request of the TEA Commissioner, the Superintendent of a K-12 organization, or the Texas Division of Emergency Management following a K-12 security incident. Would have added charter schools as eligible customers for DIR network security services. Would have repealed requirements relating to cybersecurity training requirements to only include the district's Cybersecurity Coordinator. · SB 717 was referred to the Senate Committee on Education but did not receive a hearing. HB 4944 passed the House Committee on Public Education but was not placed on the House Local Calendar.
SB 1125 HB 4552	Johnson Longoria	· Relating to DIR purchasing of IT commodity items. · Would have authorized DIR to provide products and services through the Cooperative Contracts program in demand by a single government entity. Would have defined technology services under Government Code Section 2157.068 as means services, regardless of how the fees for those services are generally charged, that: ○ Relate to the development, configuration, review, assessment, acquisition, implementation, or maintenance of ○ IT hardware, software, or services; or other routine technology services. ○ SB 1125 was referred to the Senate Committee on Business and Commerce but did not receive a hearing. ○ HB 4552 was returned to the Local and Consent Calendar Committee.
SB 1204	Paxton	· Relating to state and local government IT and information security. · SB 1204, as passed by the Senate and the House Committee on State Affairs, contained several bills; Would have: 1. Established a second information sharing and analysis organization under DIR for other states to share cybersecurity threats and best practices; 2. Required state agencies to accept digital signatures except were prohibited by law or rule;

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
		3. Required DIR to assign state agencies security ratings based on the agencies' information security risk profile; 4. Required DIR to provide options and make recommendations for improvements in the information security maturity of any state agency assigned an information security rating of below average. Permitted DIR to assist agencies in determining additional security measures that would increase the agency's information security maturity; required DIR to provide a consolidated report including agency's security assessments and recommendations for improving the state's IT infrastructure; upon reviewing the consolidated report, authorized the LBB to direct agencies to participate in the statewide technology center program; 5. Required DIR to develop and disseminate guidance for the use of distributed ledger technology, including blockchain, among state agencies; 6. Required agencies to include in their strategic plans a description of customer service technology, including telephone systems and websites, that improves customer service performance; 7. Permitted state agencies to accept peer-to-peer payments through Texas.gov and required DIR to post on its website at least three commonly used peer-to-peer payment systems that provide for data privacy and financial security; 8. Allowed state agencies to share Information Security Officers; 9. Allowed DIR to use appropriated money to market to state agencies and local governments shared information resources technology services offered by the department under this subchapter, including data center, disaster recovery, and cybersecurity services with the approval of DIR's Executive Director; 10. Allowed state agencies to use money from the Technology Improvement and Modernization fund to mitigate a security breach but prohibited it from being used to pay ransoms; and 11. Required state agencies to include an IT modernization plan as part of their state strategic plan. Permitted DIR to provide a template for the modernization plan for agencies to use. • SB 1204 passed the Senate and was placed on the House Local Calendar but was not reached before the calendar deadline.
SB 1205	Paxton	• Relating to the modernization of IT of state agencies and certain local governments. • Would have required state agencies to include an IT modernization plan in the agency strategic plan that is currently submitted each even-numbered year. Would have required the Sunset Advisory Commission to review an agency's IT modernization plan. • Would have defined peer-to-peer payments and permitted agencies to accept peer-to-peer payment systems through Texas.gov and would have required DIR to post the most commonly used peer-to-peer payment systems on DIR's website. • Would have required state agencies to accept digital signatures for communications or electronic payments delivered to the agency unless expressly prohibited by law. • Would have required DIR to develop and issue guidance for the use of distributed ledger technology and blockchain technology.

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
		· Would have required DIR to provide instructions to state agencies that require agencies to include a description of customer service technology in the technology section of their agency strategic plans. · Would have allowed DIR to use appropriated funds to market shared information resources technology including the data center, disaster recovery, and cybersecurity services to state agencies and local governments. · Would have required state agencies and local governments to use the top-level domain ".gov" or ".texas.gov" for the entity's official internet website. Would have required DIR to assist entities in obtaining a ".gov" or ".texas.gov" domain. Would have authorized DIR to establish a grant program to assist state agencies and local governments' transition to the ".gov" or ".texas.gov" domain. · SB 1205 was referred to the Senate Committee on Business and Commerce but did not receive a hearing.
SB 1986 HB 4102	Hughes Guillen	· Relating to prohibiting the acquisition or use of certain unmanned aircraft by a government entity. · Would have prohibit government entities—including DIR—from acquiring or using unmanned aircraft or any related services or equipment produced by a company that the government entity knows or has reason to believe is owned/majority-owned, held, or controlled by the government of—or headquartered in—China, Iran, North Korea, Russia, or Syria. · Would have also required DIR to add such companies to its Model Security Plan for Prohibited Technologies, as well as add companies: 1) listed in Section 889 of the federal National Defense Authorization Act, 2) excluded by future Acts of Congress or federal administrative rulemaking, or 3) deemed by DIR as unsuitable for use by a public agency. Would apply to the acquisition of unmanned aircraft or any related services or equipment on or after the bill's effective date (September 1, 2023) and to the use of an unmanned aircraft or any related services or equipment two years after the effective date. · SB 1986 was referred to the Senate Committee on Business and Commerce but did not receive a hearing. HB 4102 was referred to the House Committee on State Affairs but did not receive a hearing.
SB 2358 HB 4023	Parker Harris	· Relating to security procedures for digital applications that pose a network security risk to state agencies. · Would have required DIR to compile, maintain, and annually update a list of digital applications that create a network security risk to state agencies, and post the list on DIR's website. · Would have required DIR to develop, maintain, and periodically update a model policy for state agencies to use, limiting or prohibiting the placement and use on communication devices of any digital applications included on the digital application security risk list. · Would have required each state agency to develop, implement, and periodically update a policy limiting or prohibiting the placement and use of digital applications included on the list on: (1) state-owned cell phones, computers, and other communication devices; and (2) personal communication devices of state agency employees that are used in the agency's office or other workplace. Would have required agencies to submit to DIR a copy of the policy required and authorized DIR to offer recommendations for improvements to submitted policies.

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
		· Would have required DIR to retain each copy and to notify each member of the Legislature and the Governor when a state agency submits a policy or update. · Would have authorized DIR to adopt rules to implement this subchapter. · SB 2358 passed the Senate and was referred to the House Committee on State Affairs but did not receive a hearing.
HB 564	Raymond	· Relating to a study on energy-efficient and energy-saving information technologies. · Would have required DIR to collaborate with the Texas Facility Commission in conducting a new study to develop a strategy for state agencies to maintain, purchase, and use energy-efficient and energy-saving information technologies at state-owned and -operated facilities. · HB 564 was referred to the House Committee on State Affairs but did not receive a hearing.
HB 1413 HB 4822	Capriglione Shaheen	· Relating to the awarding of certain contracts for software, hardware, or technology services. · Would have required Shared Technology Services contracts for software, hardware, or technology services awarded under Government Code Section 2054.0565 to comply with Government Code Section 2157.068(e-1), which stipulates dollar thresholds for the minimum number of vendors who must be consulted for pricing when awarding IT commodity items. However, no contracts are awarded under Government Code Section 2054.0565; rather, that statute permits DIR to include in DIR contracts terms that allow the contracts to be used by external entities, including other state agencies, political subdivisions, etc. · HB 1413 and HB 4822 were referred to the House Committee on State Affairs but did not receive a hearing.
HB 1723	Raymond	· Relating to requiring DIR to conduct a study concerning the cybersecurity of small businesses. · Would have required DIR to conduct a study on the cybersecurity of small businesses. Would have required DIR, in collaboration with the Texas Workforce Commission, to conduct a study of how small businesses can improve cybersecurity and protect against threats to the business' supply chain and determine the feasibility of establishing a grant program for small business cybersecurity. · HB 1723 passed the House and was referred to the Senate Committee on Business and Commerce but did not receive a hearing.
HB 2494	Jetton	· Relating to Information Security Officers and network threat detection and response for state agencies. · Would have required state agencies to consider as part of their information security plan whether network threat detection and response solutions that permit anonymized security reports to be shared among participating entities in as close to real time as possible. Would have enhanced the plan and included those solutions as part of the plan as the agency determines appropriate. Would have required state agency Information Security Officers to report to DIR on security issues and to the state agency's executive management on other issues. · HB 2494 was referred to the House Committee on State Affairs but did not receive a hearing.
HB 3133	Guerra	· Relating to the electronic system for occupational licensing transactions administered by DIR.

Bill Number	Author	Summary of Key Provisions/Reason Bill Did Not Pass
		· Would have required the DIR-administered online system of occupational license transactions system to also provide a non-public way to track the status of a license holder or applicant, including disciplinary history. · HB 3133 was referred to the House Committee on State Affairs but did not receive a hearing.
HB 3217	Lujan	· Relating to a biennial audit by DIR and resources of state agency IT infrastructure. · Would have required DIR to conduct a biennial audit of each state agency's IT infrastructure. · HB 3217 was referred to the House Committee on State Affairs but did not receive a hearing.
HB 4996	Bell	· Relating to a statewide cyber insurance program. · Would have required DIR to contract with a cyber risk model vendor to conduct a study on the development of a statewide risk framework in order to determine the need for—and feasibility of implementing—a statewide cyber insurance program, and in conjunction with the State Office of Risk Management, to prepare and submit to the Governor and the Legislature a report containing the results of the study and any recommendations for legislative or other action to address the need for—and feasibility of requiring—cyber insurance. · HB 4996 was placed on the House Calendar but was not reached before the calendar deadline.

IX. Major Issues

DIR has identified the following major issues hindering the agency:

- Outdated statutory language and conflicting compliance obligations;
- Attracting and hiring talent for DIR's IT workforce; and
- Public and customer confusion regarding DIR's role in the State of Texas due to unclear departmental name.

Outdated Statutory Language and Conflicting Compliance Obligations

A. Brief Description of the Issue

Because DIR is tasked with contracting for IT goods and services, its operations are subject to one of the most rapidly changing market sectors in the world's economy. By contrast, DIR's operations are governed by statutes that may generally only be updated or modernized during the biennial meeting of the Texas Legislature.

Although several helpful changes have been made during recent legislative sessions, DIR's governing statutes have not been substantially revised since 2005. Not only has technology changed a great deal since that time, but substantial evolutions have occurred in the requirements of Texas procurement law, the scope and nature of DIR's mission and duties, and the priorities of public sector entities. These changes sometimes result in DIR facing unclear statutory guidance, conflicting legal requirements, and the inability to be agile and responsive to customer needs. In addition, the rapid pace of change in technology makes it difficult to

determine which legal authority applies to a particular state technology need and the scope of DIR's authority to respond to said need.

B. Discussion

Broad Areas of Ambiguity

At the highest level, the increasingly blurred lines between different technologies or technological approaches create various ambiguities and pose numerous interpretative difficulties across DIR's governing authorities. For example, the Legislature recently needed to clarify provisions related to "telecommunications services" in the statewide technology services program because online communication tools are increasingly being used for the functions more traditionally associated with telecommunications. Similarly, devices like police radios, electronic roadway signs, and other items not traditionally associated with IT increasingly incorporate internet connectivity and functionality akin to more traditional IT goods and services. Should technology continue with this trend, the contours of what products are properly within the scope of DIR's mission will become increasingly difficult to distinguish from items that are properly within the scope of other agencies' missions.

In addition, the changing and expanding nature to address current technology and customer needs, often at the direction of—or with approval from—the Legislature through the appropriations process, has blurred the lines between some of DIR's programs. For example, DIR operates the Managed Security Services (MSS) contract to provide cybersecurity services to a broad range of state and local entities. DIR has sufficient authority to operate the contract at present, but it does so in reliance on statutory authority drawn partly from [Government Code Chapter 2059](#),³⁶⁴ partly from [Government Code Chapter 2054](#),³⁶⁵ and partly from discrete sections of appropriations acts. With this complex web of authorities, DIR can find it difficult to determine with certainty whether DIR has the authority to provide services for any new needs that may be identified among these entities.

Specific Areas of Ambiguity

The drivers of perhaps the most difficult statutory authority ambiguities and interpretive challenges are the evolving and expanding utilization of DIR's Shared Technology Services (STS) by a wider array of customers with a broader range of needs than DIR has served in prior years; the rapid evolution of cloud computing; the market-wide shift to the "as-a-service" delivery model; and the increasing customizability of commercially available, off-the-shelf IT products, and complexity of the services necessary to configure, deploy, and support those products.

Three specific areas of statutory ambiguity or tension are particularly exacerbated by these changes. Those three areas of statutory ambiguity or tension include the current technology

³⁶⁴ [Gov't Code Chapter 2059](#).

³⁶⁵ [Gov't Code Chapter 2054](#).

marketplace, IT “commodity items,” and procurement statutes.

- **Ambiguity in the Current Technology Marketplace:** There is great potential for ambiguity in the application of [Government Code Chapter 2054, Subchapter L](#)³⁶⁶ as it applies to the current technology marketplace. DIR finds it particularly challenging to interpret and apply for the utilization of public cloud infrastructure and the “as-a-service” delivery model, in which access and use of hardware is bundled together with access and use of software or applications and sold based on a periodic subscription. Modernization of this language to reflect the move to a digital information technology landscape would be of great help.
- **Ambiguity in IT “Commodity Items”:** Similarly, there can be significant difficulty in the interpretation and application of [Government Code Chapter 2157](#)³⁶⁷ as it applies to IT “commodity items.” Because such was the norm at the time of the statute’s drafting, the language seems to assume that technology solutions can be primarily understood in terms of hardware and software, both sold under a traditional purchase and licensing model. As mentioned above, the transition to digital delivery, cloud-based infrastructure, and subscription-based “as-a-service” sales are hard to analyze under the existing statutory language. In addition, the degree to which services and support of products fit within the definition of a “commodity item,” or if such items are a proprietary or sole-source purchase, can be a challenge to determine in the increasingly segmented market for technology products.
- **Ambiguity in Procurement Statutes:** DIR finds it significantly challenging to apply Texas procurement statutes and the Texas Procurement and Contract Management Guide to individual products accessed through the Shared Technology Services (STS) programs. In general, current law assumes that the government entity acquiring and consuming goods or services will also be the entity undertaking the procurement activities for those goods and services, including initial solicitation, contract awarding, contract management, and final contract closeout. When such goods and services are necessarily procured and delivered through the shared services model that DIR is legally required to utilize for STS,³⁶⁸ tension often arises between DIR’s responsibility for compliance with procurement statutes and its obligations to generate cost and time savings for customer agencies. Additionally, compliance with some procurement statutes requires knowledge and control that rests solely with the customers DIR serves. This concern is particularly apparent with rules related to proprietary purchases.

³⁶⁶ [Gov’t Code Chapter 2054, Subchapter L](#).

³⁶⁷ [Gov’t Code Chapter 2157, Subchapter B](#).

³⁶⁸ [Gov’t Code § 2054.391](#).

C. Possible Solutions and Impacts

If the Legislature wills that DIR continues to develop its programs according to its present strategic direction, the Legislature may need to consider modernizing some of these statutes to provide additional clarity and flexibility in view of the rapid pace at which technology is changing.

Broad Revisions to Consider

The Legislature may wish to consolidate the statutes governing all of DIR's various programs under a more comprehensive chapter of the Government Code. At present, DIR operates programs enabled by numerous chapters of the Government Code³⁶⁹ and various other portions of law. Having these statutes dispersed throughout the Government Code creates questions about the degree of interconnectivity or separateness among these authorities and their related programs. Having all these statutes in a single chapter governing DIR's programs would afford greater clarity and simplify the harmonization of programs to assure they conform to the will of the Legislature and the needs of Texas.

Regarding the increasingly "IT-like" functionality of products and services not traditionally associated with IT, the Legislature may wish to consider the interpretive standard it wishes DIR and other agencies to employ when determining if an item is properly within the scope of DIR's mission and programs. One solution might be to provide rules of construction for determining how to apply statutory definitions to modern technology offerings. These offerings often contain components that cut across multiple categories of product. Applying such a rule would remove ambiguity where a technology product or service performs these "IT-like" functions only incidentally to—or in furtherance of—another unrelated primary function. Such a test could provide greater clarity and accuracy in the operations of both DIR and other state entities.

Specific Areas for Consideration

The Legislature may want to particularly consider changes related to the three specific and acute areas discussed above.

First, it may wish to consider amending [Government Code Chapter 2054 Subchapter L](#)³⁷⁰ in several ways. The statute might benefit from changing the references to "statewide technology centers," which many readers associate in context with physical brick and-mortar technology centers, rather than the programmatic centers that the state now requires. It might be helpful to instead reference "shared technology services programs" or some similar designation that more clearly identifies the scope of this authority.

³⁶⁹ Gov't Code Chapters [2054](#), [2157](#), [2170](#), and [2059](#).

³⁷⁰ [Gov't Code Chapter 2054, Subchapter L](#).

Similarly, the Legislature may wish to consider revising [Government Code Chapter 2157](#)³⁷¹ to reflect changes to the way software is sold and deployed. Commercially available software products increasingly require some degree of configuration and integration services to render them fit for a customer's needs. Therefore, the Legislature may wish to consider including such services within the definition of a "commodity item." Such change would greatly facilitate the ability of DIR's Cooperative Contracts program (COOP) to generate cost savings on the broad range of specialized or niche products and services increasingly desired by eligible entities.

In [Government Code Chapter 2157](#),³⁷² the Legislature may also wish to specify that infrastructure services and accompanying support, whether obtained through a public cloud provider or a hosted software solution, are within the meaning of "commodity item." Doing so would make clear that "as-a-service" IT products are within the scope of the program. All indications are that the software industry will continue to migrate toward that business model, so that clarification would greatly improve the longevity of the program and its responsiveness to the business needs of Texas public entities.

Finally, the Legislature may wish to consider adding clarifying language to DIR's enabling statutes that specify whether DIR, DIR's customer entities, or some combination of the two are responsible for compliance with the more difficult procurement rules. In the alternative, the Legislature may wish to clarify various procurement statutes to specify what actions by DIR or its customer entities constitute compliance with procurement rules through Shared Technology Services.

Should the statutes be revised, attention to rules related to proprietary purchases and the requisite process for commodity-item purchases within the context of the STS programs might prove especially effective at ensuring DIR is performing with both the desired efficiency and compliance excellence the Legislature rightly expects. If revisions were made recognizing these programs' unique natures and specifying the Legislature's preferred method for compliance with procurement rules in the resulting unique situations, it would greatly increase compliance efficiency and DIR's ability to provide both cost savings and responsive service to the state's IT needs.

Broad Revisions to Consider as Described by Major [Obstacles Section Above](#)

Although DIR is fortunate to have a team of highly accomplished professionals, including an excellent Office of General Counsel, the statutory ambiguities and unclear legal authorities discussed previously create substantial challenges that consume resources that otherwise could be directed to serving DIR's customers and, ultimately, the state of Texas.

³⁷¹ [Gov't Code Chapter 2157, Subchapter B.](#)

³⁷² [Gov't Code Chapter 2157.](#)

Attracting and Hiring Talent for DIR's IT Workforce

A. Brief Description of Issue

DIR experiences unique challenges in attracting, hiring, and retaining top-level talent in the technology sector, particularly in the Austin Metroplex. These workforce challenges are most apparent when DIR seeks to fill IT, network engineering, cybersecurity, and technology procurement positions.

B. Discussion

State government competes for the same talent pool as the private sector, but offers lower salaries, fewer perks, and diminished total reward offerings. According to the State Auditor's Office, the turnover rate for state employees was the highest it has ever been in FY22 at 28 percent, with 12 percent of that turnover in the IT category.³⁷³ In addition to its competition with the private sector, DIR loses talent to larger state agencies that have multi-layered tiers for career growth, higher full-time equivalent (FTE) staffing counts, and turnover savings, all of which provide greater flexibility for salary budgets and increased job offers.

C. Possible Solutions and Impacts

DIR is subject to the state's prescribed job classifications and descriptions. Although these classifications and descriptions are adapted to address the evolution of particular fields and careers, the IT industry has outpaced state descriptions for IT positions. State government should consider regularly reviewing and updating job descriptions to attract IT talent based on skills and knowledge rather than degree and certification requirements. Job descriptions should include competency-based language that highlights the required skills that are essential to the job function. State agency IT job titles, classifications, and descriptions should also align more closely to the private sector, where job descriptions and titles have already evolved to address the ever-changing needs of the IT industry. Evolving the state classifications and job descriptions to incorporate competency-based language would invite a more competitive candidate pool of technical and non-technical professionals.

Public and Customer Confusion Regarding DIR's Role in the State of Texas Due to Unclear Departmental Name

A. Brief Description of Issue

DIR's purpose as the technology leader for the state is not readily apparent from its name. Due to its statutory identification as the Department of Information Resources, DIR is often mistaken by the public as the entity that holds information comprehensively and generally for the state. In addition, customers often confuse DIR as customer support for their own IT needs.

³⁷³ State Auditor's Office, An Annual Report on Classified Employee Turnover, available at <https://sao.texas.gov/reports/main/23-703.pdf>

B. Discussion

[Government Code Chapter 2054](#) established the “Department of Information Resources” (DIR).³⁷⁴ DIR is responsible for delivering technology solutions to state and local government entities by:

- Offering purchasing support and policy insights, so organizations across all levels of Texas government can find and securely implement modern technology;
- Setting forth strategic direction for IT statewide through policies and guidance;
- Analyzing cybersecurity risks and solutions;
- Empowering state and local government entities with reliable and secure technology;
- Assisting with technology procurement and purchasing;
- Collaborating with technology vendors; and
- Creating a dynamic online community for knowledge sharing.

DIR often finds that the general public and customers are either confused by or misunderstand DIR’s role in state government due to statutory identification as the “Department of Information Resources.” Evidence of this confusion is apparent in the general communications received at AskDIR (DIR’s online question portal) through which the general public requests general information, public information requests, and other records that DIR does not possess, such as requests for criminal history information, law enforcement surveillance videos, and general legal and court case documents. Additionally, DIR receives dozens of legal filings a month on behalf of individuals seeking to have their criminal records expunged on the mistaken belief that DIR is a repository of this information.

Over the past four years, DIR has engaged in a branding campaign to educate the state on the agency’s role and mission and clarify this public confusion. This branding campaign included the creation of its Program Development Office (PDO) (now the Chief Experience Office) and redesign of its website and online presence on social media sites, such as YouTube and LinkedIn. However, DIR continues to experience misunderstandings due to the public’s perception of DIR based on its name.

Furthermore, the Legislature has expanded DIR’s role significantly since DIR’s designation as the “Department of Information Resources” in 1993.³⁷⁵ Initially, DIR provided only leadership in—and coordination of—information resources management within state government, most critical of which is the publication of strategic guidance on information resources management. Now, as described at length in III. History and Major Events and VIII. Guides to Agency Programs, DIR is tasked with an expanded number of duties including:

³⁷⁴ [Gov’t Code § 2054.004](#).

³⁷⁵ *Id.*

- Addressing cybersecurity threats to critical infrastructure and improving state agency preparedness in the event of a security incident, increasing overall cybersecurity awareness, and improving the strength of state agency cybersecurity programs;
- Increasing customer access to cost-effective, secure, and customer-oriented technology services and solutions through Shared Technology Services (STS), Cooperative Contracts program (COOP), and the Telecommunications program;
- Accelerating statewide digital transformation by providing innovative and agile solutions that transform public-sector digital capabilities;
- Strengthening public-sector data governance by providing training to expand knowledge of—and increase the adoption of—data management best practices;
- Optimizing IT procurement and contracting practices across eligible customers by offering purchasing support, so organizations across all levels of Texas government can find and implement modern, reliable, and secure technology; and
- Advancing the state’s use of—and transformation toward—innovative and emerging technologies.

With public and customer confusion regarding DIR’s role and mission, even in the face of DIR’s ongoing rebranding to address these concerns, the name statutorily granted to DIR in 1993 is no longer descriptive of DIR’s expanding responsibilities.

C. Possible Solutions and Impacts

DIR recommends changing its name as the Department of Information Resources to better align with DIR’s statutory duties as the state agency responsible for IT. This could take the form of one of the following:

- Texas Cybersecurity and Technology Agency;
- Texas Department of Information Technology; and
- Texas Department of Technology and Cybersecurity.

Changing DIR’s name would alleviate public and customer confusion about the agency’s role and responsibilities, while also addressing developments in DIR’s duties and the IT field.

While a name change may cause additional confusion in the beginning, through branding campaigns and customer outreach, DIR would be able to relieve this potential drawback fairly quickly with a name that could be more easily understood without additional context as other agencies have similarly done.

Upon a statutory name change, DIR would need to update all resources, including its website, presentations, and information pamphlets, to reflect its new name. DIR would also need to

update its administrative rules found at [1 Texas Administrative Code Part 10](#)³⁷⁶ and the name would need to be updated throughout other statutes.

D. What Key Obstacles Impede Your Agency's Ability to Achieve Its Objectives?

Network Security Information Protected by DIR

By statute, DIR is responsible for protecting the network security information of Texas state agencies, institutions of higher education, local governments, and Texans themselves.

The Legislature recognizes the need to keep network security information confidential. While the Texas Public Information Act ensures that the public has access to government records, it deems information related to computer security or infrastructure confidential and exempt from disclosure.³⁷⁷

DIR receives hundreds of public information requests throughout the course of a year. Of these, DIR receives many requests for security incidents reported to DIR by state agencies and local governments, IT modernization plans received by DIR, and other information submitted by government entities into the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM). These reports, plans, and SPECTRIM information contain in-depth network security information, which, if released, could result in unauthorized access to the state's network by threat actors.

Even though this information falls under the network security exception and must be protected, DIR must seek an Office of the Texas Attorney General Open Records Division (Open Records Division) ruling in order to withhold the information from release. The process of collecting responsive information, creating a request for ruling, and submitting the request for ruling to the Open Records Division can take DIR staff approximately 10 hours per request to complete.

Then, the Open Records Division must also issue a determination ordering DIR to withhold these network security documents before DIR can do so. While it is likely that the Open Records Division will determine that the information must be withheld, every submission to the Open Records Division that DIR makes creates an opportunity for a ruling ordering DIR to release network security information.

A statutory authorization permitting DIR to withhold confidential network security information without an Open Records Division ruling would ensure the security of this information and reallocate the resources currently addressing these requests to other necessary and important work.

³⁷⁶ [1 Tex. Admin. Code Part 10](#).

³⁷⁷ [Gov't Code § 552.139](#).

E. What, if any, agency or program functions does your agency perform that are no longer serving a clear and ongoing purpose? Which agency functions could be eliminated?

All of DIR's functions continue to serve a clear and ongoing purpose as described in Section II. Key Functions and Performance. However, the oversight function of the Information Technology Council for Higher Education (ITCHE) and several required reports could be eliminated.

Information Technology Council for Higher Education Oversight Function

Due to its role as the technology agency for the state, DIR is tasked by state law with serving other entities,³⁷⁸ including state agencies, institutions of higher education, and local governments. DIR consistently works with its customers to ensure that all programs and services meet their needs.

Institutions of higher education maintain a unique role of authority in DIR's administration through the statutorily created ITCHE,³⁷⁹ which includes the Chief Information Officers (or equivalent employee) of the Texas public university systems, such as:

- The Texas A&M University System;
- The University of Texas System;
- The Texas State University System;
- The University of North Texas System;
- The University of Houston System;
- The Texas Tech University System; and
- One institution of higher education that is not a public junior college who is selected by a majority of the other ITCHE representatives.³⁸⁰

In 2005, the Legislature passed legislation to consolidate the state's disparate data centers into two DIR-operated data centers, referred to as Statewide Technology Centers. In the same bill that charged DIR with data center consolidation, the Legislature required DIR to obtain ITCHE approval before expanding or establishing a Statewide Technology Center that includes participation by an institution of higher education, a term that includes public junior colleges for this purpose.³⁸¹ The Legislature created ITCHE only two years earlier as part of an overhaul of state agency regulations on higher education and sought to continue ensuring that DIR addressed higher education's unique technology needs. DIR's operation of the data centers was

³⁷⁸ [Gov't Code § 2054.0285\(b\).](#)

³⁷⁹ [Gov't Code § 2054.121\(b\).](#)

³⁸⁰ [Gov't Code § 2054.121.](#)

³⁸¹ [Gov't Code § 2054.377.](#)

untested and, understandably, concerns emerged over security and management.

After almost two decades, however, the consolidation of the state's data into the two highly secure, redundant data centers operated by DIR is complete, and the data centers are secure. This program has since evolved into the Shared Technology Services (STS) programs, which provide customers with new technologies and stronger security tools through contracts offering additional services. However, the requirement remains in place that institutions of higher education interested in receiving STS must obtain ITCHE's approval to use STS services. The scope and interconnectedness of STS ensure that IT and cybersecurity across the state is robust, redundant, and secure to best protect the data and technological assets of Texas. This accessible security is particularly important for entities such as public junior colleges or smaller public institutions of higher education that may wish to develop their own mature managed services but do not have access to the resources, knowledge, or expertise necessary to do so. This barrier adds complexity and time when accessing these important programs for institutions of higher education—particularly those not represented in ITCHE.

While DIR understands ITCHE's need to be aware of institutions of higher education using STS, ITCHE's approval no longer serves the same purpose as initially intended by statute, instead creating unintended roadblocks as all involved with the approval process are already heavily involved in entity operations and, as such, would be aware of their institution's pursuit of managed services through DIR. Further, institutions of higher education have a required seat on DIR's governing board which adds an additional layer of visibility and input by higher education into the operations of DIR.

In addition to the approvals required for an institution of higher education to receive STS, state law requires DIR to consult directly with ITCHE prior to adopting a proposed rule that applies to institutions of higher education. DIR must consult with ITCHE to prepare an analysis of a rule's impact on institutions of higher education. This analysis includes consideration of the rule's impact on the mission of higher education, student populations, and federal grant requirements; alternate methods of implementation to achieve the rule's purpose; and institution of higher education exemption from all or part of the requirements. DIR must also identify the public benefits expected as a result of adoption of the rule. These analyses, amongst others, must be included in the preamble of the proposed rule that is published in the *Texas Register*.³⁸²

Other than ITCHE, state law does not require DIR to consult with any state agency, local government, or other stakeholder impacted by the rule in reaching its conclusion under these analyses. DIR is the only agency subject to ITCHE's review of its rules impacting institutions of higher education, even though DIR is not the only agency whose rules apply to institutions of higher education. During a rule review or amendment, DIR works extensively with state—and local, when appropriate—government stakeholders, including state agencies and institutions of

³⁸² [Gov't Code § 2054.121](#).

higher education, before ever proposing a rule to the DIR Board of Directors. Due to the thorough conversations that DIR holds with its stakeholders, DIR typically receives information regarding the impact of a particular rule upon institutions of higher education long before it is submitted to ITCHE for consultation and review.

Because of this statutory requirement, DIR expends significant time and resources consulting with ITCHE on matters that have previously been discussed with institutions of higher education during the drafting process.

DIR values institutions of higher education input and ensures the inclusion of subject matter experts from these entities in the creation and amendments of its rules. However, the required consultation with ITCHE adds time, complexity, and unnecessary, unique formal oversight to DIR's rulemaking process. This oversight is redundant DIR includes institution of higher education representations with subject matter expertise in the specific field impacted by—or relevant to—the rule earlier in the mandatory analyses process under the Administrative Procedure Act. This process leads to a situation in which DIR finds itself subject to more extensive and interactive stakeholder requirements than imposed upon those state agencies required to determine fiscal impacts upon regulated persons.

DIR could streamline its rulemaking process if the Legislature removed enforced consultation with ITCHE and instead required DIR only to consider the enumerated elements impacting institutions of higher education as part of its Administrative Procedure Act analyses.³⁸³

Duplicative or Obsolete Reports

State law requires DIR to submit several reports to the Legislature, and requires state agencies to submit reports to DIR. While many of these reports continue to serve an ongoing purpose and provide value, some required reports, or elements of these required reports, are either duplicative or obsolete.

Reports that DIR is Required to Submit

These statutory reports (or report elements) that could be eliminated include:

- **The Data Center Services Consolidation Measurement Report.** DIR is tasked with measuring and reporting on the financial performance and progress of the data center consolidation effort.³⁸⁴ This report no longer serves a clear and ongoing purpose for two reasons. First, the data center consolidation effort was completed in July 2016, which renders the ultimate purpose of this report as met. Second, the report was intended to determine whether it was more cost-effective for Texas for customers to participate in the Data Center Services (DCS) program than to provide

³⁸³ [Gov't Code § 2054.121\(c\)-\(d\)](#).

³⁸⁴ [Gov't Code § 2054.062](#).

their own IT resources, which is difficult to directly compare due to the many variables and considerations. The Legislative Budget Board created this requirement to hold all agencies, not just DIR, accountable for completing consolidation. With that goal accomplished, this report should be eliminated—and perhaps replaced—with one that informs state leadership on current technological progress.

- **Telecommunications in the State Strategic Plan.** In the State Strategic Plan, DIR must address matters relating to a state telecommunications network for state agencies and institutions of higher education that will effectively and efficiently meet the long-term requirements of state government for voice, video, and computer communications.³⁸⁵ Subject to its statutory authority,³⁸⁶ DIR established a state telecommunications network and offers an expansive portfolio of voice and data services to eligible government entities through the Texas Agency Network (TEX-AN) program. The realization of the state telecommunications network and the TEX-AN program fulfill the condition upon which this analysis is presupposed. In addition, DIR reports on the status of the state telecommunications network and the TEX-AN program in the Biennial Report on Telecommunications. As such, this statutory requirement is no longer necessary.
- **Agency Information Resources Strategic Planning Instructions.** State law requires which are no longer necessary as state agencies are now instructed not to include an IT plan in their Agency Strategic Plan as modified by the Legislative Budget Board and Office of the Governor.³⁸⁷ Given this modification, this statute is now rendered obsolete.

Reports that Agencies are Required to Submit to DIR

In addition to those reports that DIR is required to create, state agencies must submit a number of reports to DIR. Many of these duplicate agency efforts or have conflicting submission deadlines. In addition to these concerns, DIR has little to no enforcement authority to ensure that state agencies are completing the required reports that must be submitted to—and often considered by—DIR when a report of its own must be submitted to state leadership. Many of these reports must continue to exist; however, it is critical that the report requirements be updated to reflect changes in technology, state government, and state programs and services. These reports (or report elements) include:

- **The Information Security Assessment and Report.** State agencies must³⁸⁸ complete an information security assessment of their information resources systems, network

³⁸⁵ [Gov't Code § 2054.0925.](#)

³⁸⁶ This authority is granted under [Gov't Code Chapter 2170.](#)

³⁸⁷ [Gov't Code § 2054.095.](#)

³⁸⁸ [Gov't Code § 2054.515.](#)

systems, digital data storage systems, digital data security measures, information resources vulnerabilities, and data governance program. The agency must then submit this assessment to DIR and certain state leadership, but statute specifies three separate deadlines for the state agency to report the results of its assessment to DIR and certain state leadership (upon request). Unfortunately, the statute does not specify the intent of this report, nor does it provide DIR with the power to enforce agency submission of this report. In addition, the information submitted by state agencies to DIR replicates, in large part, the information already collected by DIR pursuant to the Information Technology Infrastructure Report.³⁸⁹ Consolidating these two reports into a single assessment that DIR is required to collect from state agencies, including institutions of higher education, would be advantageous. This single report could be submitted on a single specified date, and a consolidated report could be submitted on behalf of the agencies to state leadership.

- **The Information Security Assessment of the Agency's Data Governance Program.** Statute³⁹⁰ requires a state agency to establish a data governance program that identifies the agency's data assets, exercises authority and management over them, and establishes related processes and procedures to oversee them.³⁹¹ State agencies must then biennially complete an information security assessment of their data governance program.³⁹² Information security and data governance, however, are distinct and unique programs that, while loosely connected, are not dependent upon each other. As such, an information security assessment of a data governance program would not adequately assess a data governance program. While agencies are certainly permitted to execute their own assessments, DIR is prescribed by statutory language as to what minimum requirements it may impose for an agency's analysis of its data governance program due to its inclusion as an element of the information security assessment. It would be advantageous for these two assessments³⁹³ to be statutorily separated from one another, such that the data governance review is an assessment unto itself rather than an element of the information security assessment.
- **Certain Components of the State Strategic Plan for Information Resources Management.** The State Strategic Plan provides five years of strategic goals for state agencies to follow when considering the information technology components of

³⁸⁹ [Gov't Code § 2054.068](#).

³⁹⁰ [Gov't Code § 2054.515\(a\)\(2\)](#).

³⁹¹ [Gov't Code § 2054.137\(b\)\(2\)](#).

³⁹² [Gov't Code § 2054.515\(a\)\(2\)](#).

³⁹³ Information security, pursuant to [Government Code § 2054.515\(a\)\(1\)](#), and data governance, pursuant to [Government Code § 2054.515\(a\)\(2\)](#).

their Agency Strategic Plans.³⁹⁴ This report provides necessary guidance for state agencies, allowing a unified, strategic approach to IT in the state of Texas. The State Strategic Plan must continue to exist to ensure the ongoing maturity of Texas' IT resources. However, certain sections of this report no longer contribute to this goal as they examine established service or items studied by another report. These sections include the following requirements:

- To include in DIR's analysis "interagency and interbranch communications and interagency resource sharing."³⁹⁵ DIR has enterprise services that provide for interagency communications and resource sharing, which DIR reports on in the supplemental Biennial Performance Reports. Since the implementation of these services is now complete, it is no longer necessary for DIR to make additional plans for these initiatives. DIR recommends removing the inclusion language from this provision.
- To analyze the "return on investment guidelines established by the department to help state agencies to implement major information resources projects more effectively."³⁹⁶ The Quality Assurance Team (QAT), a statutorily created group comprised of DIR, the Legislative Budget Board, and State Auditor's Office, prepares a report that includes this and other analyses of major information resources projects. DIR recommends removing this provision in its entirety.³⁹⁷
- To "outline a state information architecture that contains a logically consistent set of principles, policies, and standards to guide the engineering of state government's information technology systems and infrastructure in a way that ensures compatibility and alignment with state government's needs."³⁹⁸ DIR provides enterprise architecture through its consolidated data centers and governance, including principles, policies, and standards, through its STS programs. Since DIR implemented and completed the consolidation of the data center in 2016 and has established governance of state architecture through the Shared Technology Services programs, it is no longer necessary to make future plans for these initiatives. As this requirement is now obsolete, DIR recommends removing this provision in its entirety.

³⁹⁴ [Gov't Code § 2054.091-2054.094.](#)

³⁹⁵ [Gov't Code § 2054.091\(b\)\(1\).](#)

³⁹⁶ [Gov't Code § 2054.091\(b\)\(3\).](#)

³⁹⁷ [Gov't Code § 2054.158.](#)

³⁹⁸ [Gov't Code § 2054.092\(b\)\(2\).](#)

- To “designate and report on critical electronic government projects to be directed by the department, including a project for electronic purchasing.”³⁹⁹ DIR reports on critical electronic government projects, also known as major information resources projects, in the QAT reports required by statute,⁴⁰⁰ which renders this provision redundant. In addition, TXSmartbuy, the project for electronic purchasing referenced by this subsection, is completed. As this provision is now both redundant and obsolete, DIR recommends removing it in its entirety.
- To include in DIR’s analysis best practices for the design, deployment, and management of information resources projects “including cost benefits analysis, and staff reengineering methods to take full advantage of technological advancements.”⁴⁰¹ DIR includes best practices for the design, deployment, and management of information resources projects in the State Strategic Plan. However, this requirement is overly prescriptive and does not speak to the current state of information resources and IT as standard parts of the state agency operations. State agencies used to require significant technological guidance on every aspect of managing an information resources project, but that is no longer the case. DIR is now best situated to provide guidance on higher-level best practices in the design, deployment, and management of an information resources project, including technological and cybersecurity elements that DIR identifies as relevant or necessary. DIR recommends removing the inclusion language from this provision.
- To provide long-range policy “guidelines” for information resources in state government, “including the implementation of national, international, and department standards for information resources technologies.”⁴⁰² While DIR provides best practice guidance on the implementation of national, international, or department standards in the State Strategic Plan, DIR issues specific guidelines described by this statutory requirement through policies and administrative rules. DIR recommends amending this language to require DIR provide “guidance” rather than “guidelines” and remove the inclusion language from this provision.
- To identify the major issues faced by state agencies related to the acquisition of information resources and information resources technologies and to

³⁹⁹ [Gov’t Code § 2054.092\(b\)\(3\).](#)

⁴⁰⁰ [Gov’t Code § 2054.1183.](#)

⁴⁰¹ [Gov’t Code § 2054.092\(b\)\(4\).](#)

⁴⁰² [Gov’t Code § 2054.092\(b\)\(5\).](#)

develop a statewide approach to address the issue.⁴⁰³ DIR does include in the State Strategic Plan the major issues related to information resources technology services that state agencies face. DIR does not, however, include specific issues related to the acquisition and procurement of information resources and information resources technologies because, in coordination with the Texas Comptroller of Accounts, DIR previously established a statewide approach for acquisition of computer hardware and software including specific performance metrics for purchasing and contracting. As such, the goal of this requirement has been fulfilled, and DIR recommends removing this provision from statute.

- To identify opportunities to reuse computer software code purchased with public funds.⁴⁰⁴ This provision is outdated due to the proliferation and wide availability of modern or open-source solutions, such as Software-as-a-Service (SaaS) and low-code/no-code applications. DIR recommends removing this provision from statute.
- To identify priorities for the implementation of information resources based upon relative economic and social impacts upon the state.⁴⁰⁵ This mandate conflicts with other existing statutory requirements.⁴⁰⁶ These provisions require state agencies to identify funding priorities based on a risk analysis that includes an assessment of the business value of impacted systems and the expected return on investment, the results of which they are then required to report to DIR. Following this reporting, DIR generates a tracking code that each state agency includes in its legislative appropriations request. In addition, DIR identifies priorities for information resources technology and summarize them in aggregate in the Prioritization of Cybersecurity and Legacy System (PCLS) Report.⁴⁰⁷ DIR recommends modifying this provision to remove conflicting language about prioritizing projects based on economic or social impact and return on investment since the prioritization based on risk already includes the latter in its consideration.
- To “provide information about best practices to assist state agencies in adopting methods for design, deployment, and management of telecommunications services.”⁴⁰⁸ DIR established a state telecommunications

⁴⁰³ [Gov’t Code § 2054.092\(b\)\(6\)\(A\)](#).

⁴⁰⁴ [Gov’t Code § 2054.092\(b\)\(6\)\(B\)](#).

⁴⁰⁵ [Gov’t Code § 2054.092\(b\)\(7\)\(A\)-\(B\)](#).

⁴⁰⁶ Gov’t Code §§ [2054.069](#), [2054.572](#).

⁴⁰⁷ Gov’t Code §§ [2054.069](#), [2054.572](#).

⁴⁰⁸ [Gov’t Code § 2054.092\(b\)\(8\)](#).

network and offers an expansive portfolio of voice and data services to eligible government entities through the Texas Agency Network (TEX-AN) program as authorized by statute.⁴⁰⁹ Since DIR has implemented these services, it is no longer necessary to make additional plans for these initiatives. DIR recommends removing this provision.

- **Certain Components of the Biennial Performance Report.** This report analyzes the use of information resources technologies by state government and reports progress towards the statewide goals outlined in the State Strategic Plan.⁴¹⁰ It also includes recommendations for legislative consideration. DIR collects this information primarily through the Information Resources Deployment Review (IRDR), a self-assessment prepared by DIR and completed biennially by state agencies and reported to DIR. The Biennial Performance Report continues to be a valuable source of information for state leadership and, as such, needs to continue to exist. However, certain provisions require modification:
- **The Report on State Technology Expenditures** is an element of the Biennial Performance Report that summarizes the total expenditures for information resources and information resources technologies by the state.⁴¹¹ DIR produces this section of the report by incorporating and analyzing data from several sources to provide comprehensive estimates of state government information resources and information resources technologies expenditures. DIR outlines the data assumptions and limitations within the report but recommends adding the statutory language “based on a methodology with assumptions and limitation developed by the department” in the interest of transparency.
- **The Summary of Internet Based Training** is an element of the Biennial Performance Report that observes state agency and institution of higher education amounts and use of internet-based trainings.⁴¹² The 80th Legislature incorporated this requirement into DIR’s Biennial Performance Report in 2007 as a means to gauge the ways in which and frequency with which state agencies and institutions of higher education used the internet in their training. As reflected in the most recent data collected by DIR through the IRDR, 75 percent of state agencies, excluding institutions of higher education, reported that more than half of their training is online. In addition to the evolution of online training as the norm rather than the exception, this statute directs DIR to collect information regarding online training from institutions of higher education, which imposes a major obstacle to the collection of complete data for this report.⁴¹³ However,

⁴⁰⁹ [Gov’t Code Chapter 2170.](#)

⁴¹⁰ [Gov’t Code § 2054.055.](#)

⁴¹¹ [Gov’t Code § 2054.055\(b\)\(4\).](#)

⁴¹² [Gov’t Code § 2054.055\(b\)\(8\).](#)

⁴¹³ [Gov’t Code § 2054.055\(b\)\(8\).](#)

a different statute specifically excludes institutions of higher education from reports or plans generally mandated for a state agency under [Government Code Chapter 2054](#) unless required by DIR rule.⁴¹⁴ Any rule DIR proposed that extended a reporting requirement to institutions of higher education would be subject to ITCHE review as discussed earlier. A DIR rule identifies the specific plans and reports to which both ITCHE and DIR were able to agree applied to institutions of higher education.⁴¹⁵ DIR collects online training information through the IRDR. The list enumerated in DIR's administrative rule does not include the IRDR; therefore, although DIR promulgates the IRDR to institutions of higher education, their responses to the questions used to collect the data for this report are optional by law.

- **A Component of the Cybersecurity Report.** The Biennial Cybersecurity Report assesses the resources currently available to government entities to respond to cybersecurity incidents, identifies preventive and recovery efforts to improve cybersecurity, evaluates the statewide information security resource sharing program, and provides legislative recommendations for improving cybersecurity.⁴¹⁶ This report allows DIR to provide state leadership with information about the resources necessary and available to respond to cybersecurity incidents; as such, it continues to be a necessary element of ensuring that state leadership is aware of cybersecurity resources and limitations. However, a different statute establishes as an ongoing element of the cybersecurity report an evaluation of a program that provides an Information Security Officer to assist small state agencies and local governments that are unable to justify hiring a full-time Information Security Officer.⁴¹⁷ This provision was intended to be a one-time evaluation. DIR completed this evaluation, but the mandate still remains in statute. DIR recommends the removal of the specific element enumerated at [Government Code Section 2054.0591\(a\)\(4\)](#).⁴¹⁸

F. Aside from additional staff or funding, what are your agency's biggest opportunities for improvement in the future? For example, are there other programs or duties the agency could take on to better carry out its mission?

Establishing a statewide Chief Privacy Officer at DIR would provide a central point of contact for state agencies on data privacy matters and strategic initiatives related to data privacy. The State of Texas collects, uses, and manages vast amounts of personal, financial, and health information

⁴¹⁴ [Gov't Code § 2054.1211](#).

⁴¹⁵ [1 Tex. Admin. Code § 201.8](#).

⁴¹⁶ [Gov't Code § 2054.0591](#).

⁴¹⁷ [Gov't Code § 2054.0591\(a\)\(4\)](#).

⁴¹⁸ *Id.*

from residents to provide government information and services. Like every other state in the nation, Texas has a top cybersecurity official focused on identifying, preventing, detecting, and responding to information security and cyber threats. Now more than 20 states also have a statewide privacy role to ensure the privacy of residents' personal information is protected as well. A Chief Privacy Officer would provide a central point of contact for state agencies on best practices and policy matters involving data privacy. Employing the Chief Privacy Officer at DIR would allow seamless coordination with other statewide officials similarly at DIR (e.g., Chief Information Officer, Chief Information Security Officer for the State of Texas, and State Chief Data Officer).

X. Other Contacts

a) Fill in the following charts with updated information on people with an interest in your agency and be sure to include the most recent email address.

Texas Department of Information Resources

Exhibit 15: Contacts

Interest Groups

Communication Technology Services

Group or Association Name/ Contact Person	Address	Telephone	Email Address
AT&T/ George Spencer	208 S. Akard St Dallas, TX 75202	(512) 468-0488	gs2191@att.com
Insight/ John Brooks	10900 Stonelake Blvd Suite 20-249 Austin, TX 78759	(512) 825-0100	john.brooks@insight.com
CISCO/ Brian Steiner	18615 Tuscany Stone Suite 250 San Antonio, TX 78258	(210) 357-2504	brsteiner@cisco.com
Verizon Business/ Tory Anderson	1095 Avenue of the Americas New York, NY 10036	(940) 257-7318	tory.anderson@verizon.com
Charter/ Patrick Kufrovich	12012 North MoPac Expressway Austin, TX 78758	(512) 531-3264	patrick.kufrovich@charter.com
Hughes/ John Fanelli	11717 Exploration Ln Germantown, MD 20876	(301) 674-8644	john.fanelli@hughes.com
Lumen/ Kent Myatt	14901 FAA Blvd Ft. Worth, TX 76155	(512) 791-5368	kent.myatt@lumen.com

Cooperative Contracts

Group or Association Name/ Contact Person	Address	Telephone	Email Address
TX Public Purchasing Association (TxPPA) President/ Alan Phillips	3110 Mustang Rd Alvin, TX 77511	(281) 756-3614	aphillips@alvincollege.edu
HHSC/ Octavius Bonacquisti	4601 W. Guadalupe St Austin, TX 78751	(512) 406-2539	octavius.bonacquisti@hhs.texas.gov
TxDOT/ Ken Wood	6230 E. Stassney Ln Austin, TX 78744	(512) 416-2401	kenneth.wood@txdot.gov
TEA/ Jenna Mattingly	1701 N. Congress Ave Austin, TX 78701	(512) 463-9383	jenna.mattingly@tea.texas.gov
OAG/ Michael Gray	300 W. 15 th St Austin, TX 78701	(512) 475-4333	michael.gray@oag.texas.gov
SHI/ Renee Plemons	3828 Pecana Trl Austin, TX 78749	(512) 969-9572	renee.plemons@shi.com
Carahsoft/ Robert Moore	11493 Sunset Hills Rd Suite 100 Reston, VA 20190	(703) 871-8504	robert.moore@carahsoft.com
Accenture/ Rob Cohan	323 Congress Ave Austin, TX 78701	(512) 680-0560	robert.cohan@accenture.com
IBM/Myra Dudley	11501 Burnet Rd Building 908 Austin, TX 78758	(240) 988-7154	dudleym@us.ibm.com
CISCO/ Brian Kelly	11501 Burnet Rd Building 906, Suite 300 Austin, TX 78758	(512) 450-4615	brikell2@cisco.com
SentinelOne/ Brad Booth	444 Castro St Suite 400 Mountain View, CA 94041	(214) 578-5024	brad.booth@sentinelone.com
CrowdStrike/ Tracey Mills	206 E. 9 th St Suite 1400 Austin, TX 78701	(512) 788-1653	tracey.mills@crowdstrike.com
Oracle/ Matthew Stringer	2300 Oracle Way Austin, TX 78741	(817) 881-1772	matthew.stringer@oracle.com
Salesforce/ Kristen Casimir	950 East Paces Ferry Road NE Suite 3300 Atlanta, GA 30326	(470) 833-9061	kcasimir@salesforce.com
VMware/ Chad Lersch	6500 River Place Blvd Building 6 Austin, TX 78730	(713) 349-4120	clersch@vmware.com
Gartner/ AJ Johnson	2500 Bee Caves Rd Austin, TX 78746	(512) 426-4100	aj.johnson@gartner.com

Lobbyists

Group or Association Name/ Contact Person	Address	Telephone	Email Address
Strategic Partnerships Inc./Mary Scott Nabers	7500 Rialto Blvd Building 2, Suite 145 Austin, Texas 78735	(512) 531-3990	mnabers@spartnerships.com
Erben and Yarbrough/ Ashley Morgan	807 Brazos St Suite 402 Austin, TX 78701	(512) 663-1937	ashley@erbenyarbrough.com
DTH Strategies/ Daniel Hodge	316 W. 12 th St Austin, TX 78701	(512) 636-9136	dth@dhstrategies.com
Gregory Strategies/ David Whitley	1122 Colorado St Suite 2399 Austin, TX 78701	(512) 904-2301	david@gregorystrategies.com
Crestline Solutions/ Reed Clay	2505 Bluffview Dr Austin, TX 78704	(512) 865-0990	reed@crestline-solutions.com
Caddo Associates/ Chris Britton	919 Congress Ave Suite 1255 Austin, Texas 78701	(512) 480-0006	chris@caddoassociates.com
Bentley Public Affairs/ Matthew Bentley	1220 Colorado St Suite 450 Austin, Texas 78701	(512) 496-1085	mb@mbentley.us
Fred Shannon Governmental Affairs/ Fred Shannon	1807 Pearl St Austin, TX 78701	(512) 415-9214	fred@fredshannon.com
McGuireWoods Consulting LLC/ Holly DeShields	300 Colorado St Suite 2300 Austin, TX 78701	(512) 751-7947	hdeshields@mwcllc.com
Hillco Partners/ Neal T. "Buddy" Jones	823 Congress Ave Suite 900 Austin, Texas 78701	(512-422-0002	buddy@hillcopartners.com
The Offices of Marc A. Rodriguez/ Marc Rodriguez	1122 Colorado St Suite 2399 Austin Texas 78701	(512) 494-9798	marc@marctx.com
Jennifer Rodriguez	P.O. Box 1316 Austin, TX 78767	(512) 791-9925	jenniferrodriguez@me.com
Ray Sullivan Public Affairs/ Ray Sullivan	919 Congress Ave Suite1500 Austin, TX 78701	(512) 481-0277	ray@sullivanpublicaffairs.com
John Scott	316 W. 12 th Street Austin, TX 78701	(817) 691-5817	john.scott@scottpllc.net

Shared Technology Services Contacts

Group or Association Name/ Contact Person	Address	Telephone	Email Address
AT&T/ George Spencer	4544 S. Lamar Blvd RM MS 4401 Austin, TX 78745	(512) 468-0488	gs2191@att.com
Microsoft/ Stephen Elkins	10900 Stonelake Blvd Suite 225 Austin, TX 78759	(512) 796-3658	stelkins@microsoft.com
Dell/ John Forshay	One Dell Way Round Rock, TX 78664	(512) 924-7246	John.Forshay@Dell.com
Atos/Rudy Montoya	9500 Metric Blvd Austin, TX 78758	(512) 470-8746	rudy.montoya@atos.net
Rackspace/ Rick Rosenberg	1 Fanatical Pl Windcrest, TX 78218	(703) 909-9246	rick.rosenberg@rackspace.com
Rackspace/ Jeff Martinez	1 Fanatical Pl Windcrest, TX 78218	(571) 969-0543	jeff.martinez@rackspace.com
Amazon/ Eric LeBlanc	11501 Alterra Pkwy Austin, TX 78758	(972) 333-3435	eleblanc@amazon.com
TX Association of Business/ Massey Villarreal	316 W 12 th St Suite 102 Austin, Texas 78703	(713) 201-8879	Massey@ptg.com
Capgemini/ Ken Sinclair	600 Center Ridge Dr Suite 600 Austin, TX 78753	(512) 633-6588	Ken.sinclair@capgemini.com
Capgemini/ Kenny Wilson	600 Center Ridge Dr Suite 600 Austin, TX 78753	(425) 786-7470	Kenny.Wilson@capgemini.com
Google/ Jack O'Connell	500 West 2 nd St Austin, TX 78701	(512) 739-2911	Jackoconnell@google.com
Deloitte/ Chris Keel	500 West 2 nd St Austin, TX 78701	(512) 797-7566	Ckeel@deloitte.com
Deloitte/ Mike Wyatt	500 West 2 nd St Austin, TX 78701	(512) 771 8062	miwyatt@deloitte.com
Azure/ Stephen Elkins	10900 Stonelake Blvd Suite 225 Austin, TX 78759	(512) 796-3658	stelkins@microsoft.com

Group or Association Name/ Contact Person	Address	Telephone	Email Address
Azure/ Justin Roan	10900 Stonelake Blvd Suite 225 Austin, TX 78759	(512) 740-7159	Jroan@microsoft.com
SAIC/ Michael Fitch	11100 Metric Blvd Suite 200A, Austin, TX 78758	(415) 609-8850	michael.s.fitch@saic.com
Tyler Tech/ Patrick Wood	1122 S Capital of Texas Hwy Suite 304 West Lake Hills, TX 78746	(203) 545-7057	patrick.wood@tylertech.com
Xerox/ John Heatley	6836 Austin Center Blvd Suite 300 Austin, TX 78731	(469) 400-7366	john.heatley@xerox.com

Interagency, State, or National Associations

Group or Association Name/ Contact Person	Address	Telephone	Email Address
NASCIO/ Doug Robinson	201 E. Main St Lexington, KY 40507	(859) 514-9153	drobinson@NASCIO.org
CISA/ Ernesto Ballesteros	245 Murray Ln Washington, D.C. 20528	(210) 202-6646	ernesto.ballesteros@cisa.dhs.gov
Indiana/ Tracy Barnes	100 N. Senate Ave Rm N758-ES Indianapolis, IN 46204	(317) 232-3172	tbarnes@iot.in.gov
Nevada/ Tim Galluzi	100 N. Stewart St Suite 100 Carson City, Nevada 89701	(775) 684-5898	tim.galluzi@it.nv.gov
North Carolina/ Jim Weaver	P.O. Box 17209 Raleigh, NC 27619	(919) 809-3845	james.weaver@nc.gov
Arizona/ J.R. Sloan	100 N 15 th Ave Suite 302 Phoenix, AZ 85007	(602) 281-0394	jr.sloan@azdoa.gov
Ohio/ Katrina Flory	30 E. Broad St Columbus, Ohio 43215	(614) 995-5466	katrina.flory@das.ohio.gov
Tennessee/ Stephanie Dedmon	312 Rosa L. Parks Ave Nashville, TN 37243	(615) 516-1083	stephanie.dedmon@tn.gov

Group or Association Name/ Contact Person	Address	Telephone	Email Address
Wisconsin/ Trina Zanow	P.O. Box 7840 Madison, WI 53707	(608) 261-7750	trina.zanow@wisconsin.gov
Georgia/ Shawnzia Thomas	47 Trinity Ave SW Atlanta, GA 30334	(404) 463-2340	shawnzia.thomas@gta.ga.gov
e.Republic/ Teri Takai	100 Blue Ravine Rd Folsom, CA 95630	(916) 932-1473	teri.takai@erepublic.com

Liaisons at Other State Agencies

Agency Name / Relationship / Contact Person	Address	Telephone	Email Address
HHSC/ Cecile Young	4601 W. Guadalupe St Austin, TX 78751	(512) 424-6502	cecile.young@hhs.texas.gov
HHSC/ Maurice McCreary	4601 W. Guadalupe St Austin, TX 78751	(512) 424-6860	cts_chief_operating_office@hhsc.state.tx.us
HHSC/ Cassie Jordan	4601 W. Guadalupe St Austin, TX 78751	(512) 243-4909	cassie.jordan@hhs.texas.gov
DSHS/ Roberto Beaty	1100 West 49th St Austin, Texas 78756	(512) 298-9820	roberto.beaty@dshs.texas.gov
TxDOT/ Anh Selissen	125 E. 11th St Austin, TX 78701	(737) 235-9618	anh.selissen@txdot.gov
OAG/ Tina McLeod	209 W 14 th St, Austin, TX 78701	(512) 475.4616	tina.mcleod@oag.texas.gov
TWC/ Ed Serna	101 E. 15th St Austin, Texas 78778	(512) 463-0735	edward.serna@twc.state.tx.us
Water Development Board/ Brooke Paup	1700 North Congress Ave Suite 610B Austin, TX 78701	(512) 971-5017	brooke.paup@twdb.texas.gov
DPS/ Bryan Lane	5805 North Lamar Blvd Austin, TX 78752	(512) 750-1072	bryan.lane@dps.texas.gov
DMV/ Daniel Avitia	4000 Jackson Ave Austin, TX 78731	(512) 465-3001	daniel.avitia@txdmv.gov
TDLR/ Mike Arismendez	920 Colorado St Austin, TX 78701	(512) 463-3170	mike.arismendez@tdlr.texas.gov
TDI/ Cassie Brown	1601 Congress Ave Austin, TX 78701	(512) 676-6022	cassie.brown@tdi.texas.gov
TDCJ/ Tina Clark	209 West 14 th St Austin, TX 78701	(936) 437-1270	tina.clark@tdcj.texas.gov
SOS/ Joe Esparza	1019 Brazos St Austin, TX 78701	(512) 463-5770	jesparza@sos.texas.gov
TPWD/ Jamie McClanahan	4200 Smith School Rd Austin, TX 78744	(512) 389-8066	jamie.mcclanahan@tpwd.texas.gov

Agency Name / Relationship / Contact Person	Address	Telephone	Email Address
TEA/ Melody Parrish	1701 N. Congress Ave Austin, TX 78701	(512) 463-2321	melody.parrish@tea.texas.gov
TABC/ George Stolard	5806 Mesa Dr Austin, TX 78731	(512) 206-3458	george.stolard@TABC.texas.gov
TCOLE/ John Beauchamp	6330 East Hwy 290 Suite 200 Austin, TX 78723	(512) 936-7771	john.beauchamp@tcole.texas.gov
Texas Racing Commission/ Amy Cook	1801 Congress Ave Suite 7.600 Austin, TX 78701	(512) 840-8134	acook@txrc.texas.gov
Texas Funeral Service Commission/ James White	1801 Congress Ave Suite 11.800 Austin, TX 78701	(512) 936-2472	james.white@tfsc.texas.gov
Texas Higher Education Coordinating Board/ Sarah Keyton	1801 Congress Ave Suite 12.200 Austin, TX 78701	(512) 427-6566	commissioner@highered.texas.gov
Angelo State University/ Doug Fox	2601 W. Ave N San Angelo, TX 76909	(325) 227-9347	doug.fox@angelo.edu
UT Austin/ Andrea Sheridan	110 Inner Campus Dr Austin, TX 78712	(512) 773-1584	andrea.sheridan@austin.utexas.edu
CSEC/Kelli Merriweather	1801 Congress Ave Suite 11.100 Austin, TX 78701	(512) 305-6938	kelli.merriweather@csec.texas.gov
CPA/ Phillip Ashley	111 East 17th St Austin, Texas 78774	(512) 463-4275	phillip.ashley@cpa.texas.gov

XI. Additional Information

- a) Texas Government Code, Section 325.0075 requires agencies under review to submit a report about their reporting requirements to Sunset with the same due date as the SER. Include a list of each agency-specific report that the agency is required by statute to prepare and an evaluation of the need for each report based on whether factors or conditions have changed since the statutory requirement was put in place. Please do not include general reporting requirements applicable to all agencies, reports that have an expiration date, routine notifications or notices, posting requirements, federally mandated reports, or reports required by G.A.A. rider. If the list is longer than one page, please include it as an attachment.

Texas Department of Information Resources

Exhibit 16: Evaluation of Agency Reporting Requirements

DIR will provide Exhibit 16 as a separate attachment to this Self-Evaluation Report.

- b) Does the agency's statute use "person-first respectful language" as required by Texas Government Code, Section 325.0123? Please explain and include any statutory provisions that prohibit these changes.

To the extent that DIR references persons with mental illnesses or other disabilities, person-first respectful language is utilized.

- c) Please describe how your agency receives and investigates complaints about the agency and its operations.

DIR has limited interaction with the general public, as most of its external interactions are with either:

- Current or potential vendors of IT products or services; or
- Public or private sector entities who are eligible to utilize DIR contracts or obtain services through its shared technology programs.

However, like many state agencies, DIR is required to maintain methods for the public to submit its comments or complaints. DIR established six primary ways for the public to submit complaints about the agency or its operations directly to DIR:

1. At the conclusion of a procurement process overseen by DIR, a respondent to the procurement may file a formal protest of the awards of a DIR contracts. This is in addition to the vendor debriefings that DIR conducts for unsuccessful respondents post-award.
2. DIR actively solicits customer satisfaction feedback from the public sector entities it serves through a variety of survey tools and DIR's governance structure.
3. The DIR Board appoints a Customer Advisory Committee that reports to and advises the board on the status of DIR's delivery of critical statewide services.

4. The DIR Board accepts public comment at each public board meeting, during which time members of the general public are afforded the opportunity to address any issue of concern directly with the governing board.
5. Members of the public may submit suggestions or complaints through a designated email address (askDIR@dir.texas.gov), through our website, or in person, by telephone, or through email or mail directly to a DIR employee.
6. Any person may make a complaint to DIR's Internal Auditor or the State Auditor's Office if they believe fraud, waste, or abuse is taking place at DIR.

A more detailed description of these processes is below.

DIR is subject to Texas requirements and must post the notice entitled "[Equal Employment Opportunity Is the Law](#)," which contains information about the Equal Employment Opportunity and Americans with Disabilities Act laws.

Procurement Protests

As required by Texas Government Code Section 2155.076, DIR established a formal procedure for bid protests by administrative rule.⁴¹⁹ Any actual or prospective bidder, offeror, or contractor claiming to have been aggrieved by a contract solicitation, evaluation, or award may formally protest the action by providing a sworn written notice that includes:

1. A specific identification of the statutory or regulatory provisions that the action complained of is alleged to have violated;
2. A specific description of each act alleged to have violated the statutory or regulatory provisions that the complainant alleges DIR to have violated;
3. A precise statement of the relevant facts and an identification of the issues to be resolved; and
4. An argument and authorities in support of the protest.

The complainant must submit their sworn written notice to DIR's Chief Procurement Officer within 10 business days after the protesting party knows or should have known of the occurrence of the action being protested. The protesting party must mail or deliver copies of the protest to the department and all respondents who have submitted bids, proposals, or offers for the contract involved.

Upon receipt of a protest that meets the above-stated minimum requirements, DIR's Chief Procurement Officer will investigate and make a ruling on the protest. The Chief Procurement Officer may consult with legal counsel during this process. DIR may also solicit written responses to the protest from other bidders and interested parties. The Chief Procurement Officer may work with the protesting party to resolve the dispute by voluntary agreement; if DIR and the vendor are unable to resolve the dispute in this way, the Chief Procurement Officer must issue a formal written determination on the protest.

⁴¹⁹ [1 Tex. Admin. Code § 201.1](#).

If the protest is denied, the protestor may appeal the determination to DIR's Executive Director, who may either:

- Review the protest petition and issue a written determination; or
- Refer the matter to DIR's Board of Directors for consideration at a regularly scheduled open meeting.

In either case, the judgment rendered on the appeal is final and is DIR's final administrative action.

Customer Satisfaction Surveys

Providing excellent customer service is at the heart of DIR's mission and core values. DIR's various stakeholders and customers represent all levels of government, including state agencies, institutions of higher education, judicial organizations, local governments, school districts, quasi-government organizations, and public entities outside of Texas.

Government Code Chapter 2114 requires DIR to submit a report on the quality of its delivered services to the Office of the Governor and Legislative Budget Board by June 1 of each even-numbered year.⁴²⁰ To gather the information that informs this report, DIR sends a biennial customer satisfaction survey to all recorded customer entities, totaling 2,809 contacts in 2022. In 2022, DIR began including this same customer satisfaction survey in every monthly customer newsletter that is sent to its over six thousand contacts for more continuous and updated feedback on DIR's programs and services.

In addition to the general surveys shared with DIR customers, DIR conducts a specific analysis of customer satisfaction within STS and the various programs that it provides. Each January, the STS measures customer satisfaction for the previous calendar year. A third-party vendor conducts a comprehensive survey, which covers all topics required under the STS services agreement as well as additional areas of interest; once the third party collects and collates the data, the results are then provided to DIR, who reviews and shares the information with participating customers. STS customers also complete a monthly balanced scorecard, providing feedback to DIR on service provider performance on a more consistent schedule, allowing DIR to address services issues on a more immediate timetable.

DIR conducts annual satisfaction surveys with customers about their familiarity with DIR's programs, including the types of offerings, staff knowledge, and customer service. DIR also surveys Capitol Complex Telephone System (CCTS) and Texas Agency Network (TEX-AN) customers to determine their level of satisfaction with telecommunications services; the CTS team provides customers with a survey link through emails exchanged with customers during the course of routine work activities.

⁴²⁰ [Gov't Code § 2114.002](#).

Customer Advisory Committee

Following the conclusion of the Commission's last review of DIR in 2013, the Legislature passed HB 2472, which requires the DIR Board to appoint a Customer Advisory Committee.⁴²¹ The Customer Advisory Committee objectives are to:

- Provide input on customer experience with DIR services.
- Assist DIR in developing priorities from a statewide perspective.
- Assist DIR in implementing programs that meet customer interests.
- Advise DIR on how to consistently improve delivery of DIR services.

Members of the Customer Advisory committee represent a cross-section of organization types, professional roles of those serving on the committee, and geographic areas across the state. The committee includes representatives from local government, institutions of higher education, state agencies with fewer than 100 employees, and the public.

Public Comments Made to the DIR Board

The DIR Board meets at least quarterly with other meetings scheduled as needed to consider special topics that cannot await consideration at the next quarterly meeting. All such meetings are conducted in accordance with the Texas Open Meetings Act,⁴²² which requires to post a public notice to the *Texas Register* in advance of the open meeting to notify the public of the topics that will be taken before the Board at the open meeting and of their opportunity to provide public comment at the end of the Board meeting. The DIR Board is required to:

- Provide the public an opportunity to speak to any issue within DIR's authority at these open meetings;
- Provide the public with information about the functions of DIR;
- Maintain a complaint procedure; and
- Retain certain minimum documentation related to any complaints received.⁴²³

At the beginning of a DIR Board meeting, the DIR Board chair reviews the Board's reasonable rules regarding the public's right to address the board during the open meeting, which, among other matters, identifies the total amount of time that a member of public may address the board on a given item.⁴²⁴ It is the standard practice of the DIR Board to include a time at the end of each board meeting when the public can share testimony or comments, including complaints about DIR or its operations.

Any such complaint made in this way could be investigated in a manner that the DIR Board deems appropriate, either by the DIR Board as a whole or through an assigned subcommittee

⁴²¹ [Acts 2013, 83rd Leg., R.S., ch. 48 \(H.B. 2472\), § 4, 2013 Tex. Sess. Law Serv. 98, 99 \(codified at Gov't Code § 2054.0331\).](#)

⁴²² [Gov't Code Chapter 551.](#)

⁴²³ [Gov't Code § 2054.035; Gov't Code § 2054.036.](#)

⁴²⁴ [Gov't Code § 551.007\(c\).](#)

or a subcommittee created for the purpose of the investigation.

Customer Complaints or Suggestion through DIR Website

DIR identified its customer service principles and associated complaint procedures on DIR's website. If a member of the public wants to submit a suggestion or complaint to DIR, DIR accepts this information by email at askdir@dir.texas.gov or permits its submission in person, by telephone, by electronic mail, or in writing to any DIR employee.⁴²⁵ A [contact list for DIR program areas](#), including the appropriate email address or telephone number, is made available on DIR's website.⁴²⁶ DIR must respond to all complaints directed against the agency within one business day and have a resolution completed within one week.⁴²⁷

Reporting Fraud, Waste, Theft and Abuse

The DIR Board appoints an Internal Auditor that reports directly to the Board, who seeks to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. The Internal Auditor serves as an independent and objective source for information about agency operations, efficiency, compliance, and risk. Along with DIR's General Counsel, DIR's Internal Auditor is also available to all DIR staff or members of the public who wish to report suspected fraud, waste, theft, or abuse connected with DIR or its operations.

DIR details its process by which DIR employees may report fraud, waste, theft, or abuse in the Ethics Policy.

DIR also provides training and information to its employees about reporting suspected fraud, waste, or abuse directly to the State Auditor's Office.

d) Fill in the following chart detailing information on complaints received about your agency and its operations. Do not include complaints received about people or entities you regulate.

DIR has not received any complaints about our agency through the formal process established through the DIR website. DIR has received vendor protests, as shown in Exhibit 17 below.

⁴²⁵ Compact with Texans -Texas Department of Information Resources, <https://dir.texas.gov/site-policies/compact-texans> (last visited Aug. 18, 2023).

⁴²⁶ Contact DIR - Texas Department of Information Resources, <https://dir.texas.gov/contact-dir> (last visited Aug. 18, 2023).

⁴²⁷ Compact with Texans -Texas Department of Information Resources, <https://dir.texas.gov/site-policies/compact-texans> (last visited Aug. 18, 2023).

Texas Department of Information Resources

Exhibit 17: Complaints Against the Agency (Vendor Protests) – Fiscal Years 2018-22

	FY2018	FY2019	FY2020	FY2021	FY2022
Number of complaints received	1	0	1	1	1
Number of complaints resolved	N/A	N/A	N/A	N/A	N/A
Number of complaints dropped/found to be without merit	N/A	N/A	N/A	N/A	N/A
Number of complaints pending from prior years	N/A	N/A	N/A	N/A	N/A
Average time period for resolution of a complaint	3 months	N/A	3 months	3 months	3 months

e) Fill in the following charts detailing your agency's Historically Underutilized Business (HUB) purchases. Sunset is required by law to review and report this information to the Legislature.

Texas Department of Information Resources

Exhibit 18: Purchases from HUBs

Fiscal Year 2020

Category	Total \$ Spent	Total HUB \$ Spent	Percent	Agency Specific Goal*	Statewide Goal
Heavy Construction	N/A	N/A	N/A	N/A	11.2%
Building Construction	N/A	N/A	N/A	N/A	21.1%
Special Trade	\$1603	\$0	0%	32.9%	32.9%
Professional Services	\$0	\$0	0%	23.7%	23.7%
Other Services	\$13,741,151	\$4,904,272	35.69%	26.0%	26.0%
Commodities	\$4,585,897	\$1,785,750	38.94%	21.1%	21.1%
Total	\$18,328,652	\$6,690,022	36.50%		

DIR does not have spending in Heavy Construction or Building Construction, therefore we do not have goals for those categories.

Fiscal Year 2021

Category	Total \$ Spent	Total HUB \$ Spent	Percent	Agency Specific Goal	Statewide Goal
Heavy Construction	N/A	N/A	N/A	N/A	11.2%
Building Construction	N/A	N/A	N/A	N/A	21.1%
Special Trade	\$0	\$0	0%	32.9%	32.9%
Professional Services	\$0	\$0	0%	23.7%	23.7%
Other Services	\$16,948,407	\$6,936,017	40.92%	26.0%	26.0%
Commodities	\$7,230,381	\$6,875,492	95.09%	21.1%	21.1%
Total	\$24,178,789	\$13,811,510	57.12%		

Fiscal Year 2022

Category	Total \$ Spent	Total HUB \$ Spent	Percent	Agency Specific Goal	Statewide Goal
Heavy Construction	N/A	N/A	N/A	N/A	11.2%
Building Construction	N/A	N/A	N/A	N/A	21.1%
Special Trade	\$974	\$0	0%	32.9%	32.9%
Professional Services	\$0	\$0	0%	23.7%	23.7%
Other Services	\$28,097,306	\$9,123,896	32.47%	26.0%	26.0%
Commodities	\$9,408,171	\$1,811,358	19.25%	21.1%	21.1%
Total	\$37,506,450	\$10,935,253	29.16%		

f) Does your agency have a HUB policy? How does your agency address performance shortfalls related to the policy? (Texas Government Code, Section 2161.003; TAC Title 34, Part 1, Rule 20.286c)

Yes. If DIR experiences a performance shortfall in its HUB usage, then the HUB Program Outreach and Training team would review DIR's expenditures to determine where DIR could alter its spending to support its HUB goals, identify appropriate outreach and education opportunities to increase HUB awareness across the state, and draft a strategy specifically targeted to increase HUB usage. The team would then work closely with DIR executive management to execute this strategy in an intentional way to increase use of HUB vendors.

g) For agencies with contracts valued at \$100,000 or more: Does your agency follow a HUB subcontracting plan to solicit bids, proposals, offers, or other applicable expressions of interest for subcontracting opportunities available for contracts of \$100,000 or more? (Texas Government Code, Section 2161.252; TAC Title 34, Part 1, Rule 20.285)

Yes. All internal and statewide procurements with an expected value of \$100,000 or more require respondent vendors to submit a completed HUB Subcontracting Plan (HSP) as part of their response. All COOP program RFOs require respondents to submit a completed HUB Subcontracting Plan (HSP) as part of their response.

h) For agencies with biennial appropriations exceeding \$10 million, answer the following HUB questions.

Do you have a HUB coordinator? If yes, provide name and contact information. (Texas Government Code, Section 2161.062; TAC Title 34, Part 1, Rule 20.296)

Yes. DIR's HUB Coordinator's contact information is provided below.

Name: Lynn Hodde Blue

Title: Deputy Chief Procurement Officer

Location: William P. Clements Bldg., 300 W. 15th Street, Suite 1300, Austin, TX 78701

Office Number: (512) 463-9813

Email: lynn.hodde@dir.texas.gov

i) Has your agency designed a program of HUB forums in which businesses are invited to deliver presentations that demonstrate their capability to do business with your agency? (Texas Government Code, Section 2161.066; TAC Title 34, Part 1, Rule 20.297)

Yes. DIR also hosts DIR Connect in which HUB vendors are invited to participate in roundtables with current contract holders to understand and identify possible subcontracting opportunities with these vendors.

DIR coordinates annually with the Texas Comptroller of Public Accounts' Statewide HUB Program to cosponsor events that educate and inform customers on how to use the HUB Program. DIR also coordinates with other agencies and minority trade organizations to educate the HUB vendor community on "Doing Business with DIR."

j) Has your agency developed a mentor-protégé program to foster long-term relationships between prime contractors and HUBs and to increase the ability of HUBs to contract with the state or to receive subcontracts under a state contract? (Texas Government Code, Section 2161.065; TAC Title 34, Part 1, Rule 20.298)

Yes. As early as 2013, DIR began actively expanding its mentor-protégé program to foster relationships between HUB firms and other businesses to grow in areas they need help.

k) Fill in the charts below detailing your agency's Equal Employment Opportunity (EEO) statistics. Sunset is required by law to review and report this information to the Legislature. Please use only the categories provided below. For example, some agencies use the classification "paraprofessionals," which is not tracked by the state civilian workforce. Please reclassify all employees within the appropriate categories below.

Texas Department of Information Resources

Exhibit 19: Equal Employment Opportunity Statistics

Officials/Administration

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	43	7%	8.5%	9%	24.7%	40%	41.7%
2021	55	7%	8.5%	9%	24.7%	49%	41.7%
2022	58	7%	8.5%	10%	24.7%	48%	41.7%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

Professional

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	106	17%	10.9%	23%	21.8%	61%	54.1%
2021	109	17%	10.9%	22%	21.8%	60%	54.1%
2022	123	17%	10.9%	21%	21.8%	58%	54.1%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

Technical

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	37	19%	15.1%	5%	29.8%	19%	56.9%
2021	25	28%	15.1%	20%	29.8%	12%	56.9%
2022	25	24%	15.1%	12%	29.8%	16%	56.9%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

Administrative Support

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	6	33%	14.6%	17%	36.5%	67%	74.7%
2021	9	33%	14.6%	11%	36.5%	56%	74.7%
2022	6	67%	14.6%	17%	36.5%	100%	74.7%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

Service/Maintenance

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	0	0%	13.3%	0%	53.0%	0%	54.0%
2021	1	0%	13.3%	0%	53.0%	0%	54.0%
2022	1	0%	13.3%	0%	53.0%	0%	54.0%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

Skilled Craft

Year	Total Number of Positions	Percent African-American	Statewide Civilian Workforce Percent	Percent Hispanic	Statewide Civilian Workforce Percent	Percent Female	Statewide Civilian Workforce Percent
2020	0	0%	11.5%	0%	52.3%	0%	14.0%
2021	0	0%	11.5%	0%	52.3%	0%	14.0%
2022	0	0%	11.5%	0%	52.3%	0%	14.0%

Source for Years 2020 and 2022: [Agency Workforce Plan](#)

I) Does your agency have an equal employment opportunity policy? How does your agency address performance shortfalls related to the policy?

DIR provides equal employment opportunities to all employees and applicants. DIR does not exclude anyone from consideration for recruitment, selection, training, appointment, promotion, retention, or any other personnel action, or deny any benefits or participation in programs or activities which it sponsors on the grounds of race, color, national origin, gender, religion, age, disability, or pregnancy and related medical conditions.

In addition to federal law requirements, DIR complies with Texas Labor Code Sections 21.452, 21.502, through the development and implementation of a recruitment plan to recruit and select qualified African Americans, Hispanic Americans, and females based upon workforce

availability analyses as well as personnel selection procedures that incorporate a workforce diversity program.

DIR is committed to providing employees and applicants with fair and equal treatment. The People and Culture Office communicates the agency's commitment in the Employee Handbook, Careers website, required bi-annual training, and during new hire orientation. Employees who violate the equal employment opportunity policy are subject to disciplinary action up to and including termination.

XII. Agency Comments

a) Provide any additional information needed to gain a preliminary understanding of your agency.

DIR ensures that government entities—including state agencies, public colleges and universities, local governments, and K-12 education entities—can deliver the most secure, innovative, and cost-effective technology solutions available that allow all levels of Texas government to develop partnerships and approaches that invest in advanced public sector IT while facing the realities of budgetary constraints. Through DIR's programs, the public sector can access IT solutions that are scalable and efficient without sacrificing security.

DIR is the closest thing to privatized IT in the country. Despite being a mid-size state agency with approximately 250 current full-time employees, DIR provides essential services statewide and plays a crucial role in the strategic development of the state's technology resources. This crucial role involves providing the security that protects the state, negotiating and executing master contracts that allow public sector entities access to it, employing three⁴²⁸ statutory statewide Chief positions that provide statewide leadership, and ensuring continuous technological innovation across Texas. These accomplishments are particularly notable when comparing DIR's full-time equivalent numbers to other agencies that have similar financial and responsibility footprints. DIR currently has legislative authority for 267 full-time equivalents but operates the seven functions listed in this report within these minimal narrow staffing parameters.

DIR Stakeholders

DIR is unique because of the customers that we serve. Instead of providing services directly to the public, we serve the entities that serve the public. Texans expect and deserve the very best from their government. Therefore, DIR must provide the very best to its customers, a term that includes 98 state agencies, 70 institutions of higher education, 15 judicial organizations, and over 6,200 local government entities, to ensure that Texans' government can meet and exceed

⁴²⁸ The three statutory statewide employees are the [Chief Information Officer](#), [Chief Information Security Officer](#), and [Chief Data Officer](#).

their expectations.

Now, more than ever, government entities face fiscal constraints that demand greater levels of value from their technology purchases. The statewide reach of DIR's programs ensures that savings realized through these programs return to the State of Texas and, ultimately, its taxpayers.

Statewide Impact

At DIR, we partner with state and agency leadership to evaluate and prioritize the top technology needs of Texas. As the only state agency with knowledge of every Texas state agency's technology uses and needs, DIR is tasked by the Texas Legislature with assisting in crafting practical statewide IT policy that addresses Texas' needs by requiring DIR to submit legislative recommendations for future technology-related legislative actions in several statutorily required reports.

Additionally, the Legislature entrusts DIR with the employment of key statewide technology roles, such as the statewide Chief Information Security Officer, the statewide Chief Data Officer, and the state's Chief Information Officer.

Through our various programs, DIR helps set the strategic direction for technology statewide.

Statewide Response

DIR plays a critical role in the state's response to disasters, both natural and man-made.

During natural disasters, state leadership has historically called upon DIR to assist with telecommunications and technology needs, and ensure that state agencies and Texans have continued access to these important and necessary services during tumultuous times.

DIR is a state and federal leader in responding to cyberattacks. This leadership is most visible through DIR's handling of the state's successful response and implementation of the Cyber Annex to address the 2019 ransomware attack that affected 23 local governments across Texas.

DIR aids local governments in preparing and planning for incident responses in the event of a cyberattack. Additionally, DIR provides immediate cybersecurity response through our Cybersecurity Incident Response Team (CIRT), the Volunteer Incident Response Team (VIRT), and the Regional Security Operations Centers (RSOCs). DIR's Network Security Operations Center (NSOC) also blocks billions of intrusion attempts on the state's network every day. We provide critical training and outreach to help Texans avoid destructive cyberattacks.

Finally, as observed with the COVID-19 pandemic, DIR is instrumental in the continuity of state operations by ensuring that organizations across all levels of state and local government can find, procure, and securely implement the technologies needed to transition to remote work and the online delivery of services to Texans. DIR has partnered with other state agencies to provide application and infrastructure support when delivering critical services to Texans in challenging times. DIR has worked with state agencies throughout Texas to deploy thousands of laptops, set up websites, and develop applications to meet the needs of Texans and share

valuable information. For example, DIR utilized the existing Technology Solution Services (TSS) contract to modernize five Texas Department of State Health Services' applications improving their response and utilization of data and their ability to efficiently inform state leadership during the COVID-19 outbreak. Using TSS to complete these upgrades, the Texas Department of State Health Services' avoided using emergency procurements when upgrading and modernizing their applications, and these projects met targeted budget and completion timelines.

DIR as an Agency

While DIR may be a technology agency, we're an agency powered by people who are fiercely dedicated to our mission and vision. DIR's culture is truly one of a kind, and we are considered a model for the state in cultivating a culture that values its employees and their unique contributions. This culture invites employees to engage actively with DIR's mission and display its ILEAD values each and every day when creating excellent work products, the results of which can be observed at every level of Texas government.

DIR has received accolades for its commitment to its culture. Although we have competed against both private and public entities in the Austin area, DIR received the Austin American-Statesman Top Workplaces Award three years in a row. Additionally, DIR's work and culture has been recognized at more than just the city level; DIR has received recognition at the national level as well. In 2023, for the first time in our history, DIR received national recognition as a Top U.S. Workplace, an award that recognizes companies for making the "world a better place to work by prioritizing a people-centered culture and giving employees a voice."⁴²⁹ By giving our people a voice and actively engaging them in DIR's mission, DIR facilitates an excellent workplace that creates and innovates to the state's advantage.

DIR is the cornerstone of public sector technology in the state of Texas.

DIR Videos

DIR provides the following videos for more information on our culture, programs, and services.

- **DIR ILEAD:** https://youtu.be/6xrsAPRNW9k?si=DP_ho6IM7Y4alHbt.
- **DIR People and Culture:**
https://www.youtube.com/playlist?list=PL_QXqY3YNV7Peonel1Mlos3T0d-MCRLDw.
- **DIR Overview:**
https://www.youtube.com/watch?v=nLvG2v2An14&list=PL_QXqY3YNV7M-RAO0NDnBHqOA1GDP2B-&index=3.

⁴²⁹ Top Workplace USA 2023 (<https://topworkplaces.com/award/top-workplaces-usa/2023/>).

- **Cybersecurity:**
https://www.youtube.com/playlist?list=PL_QXqY3YNNV7OnvMj3raAFFokOs8MRuiRf.
- **Cybersecurity Awareness Training:**
https://youtu.be/YFRK_slmKkQ?si=tWeY5fpM63iv89YH.
- **Data Literacy Program:** https://www.youtube.com/playlist?list=PL_QXqY3YNNV7O6-yGmVFp_FhrhSuiFXyHT.
- **HUB Program:**
https://www.youtube.com/playlist?list=PL_QXqY3YNNV7NTtLwQMRdsQMfiUMhIWxp-.
- **IT Procurement and Contracting:**
https://youtu.be/FSbLf_aA4CU?si=nNOovGAwoLLPKPOb.
- **Information Security Forum:** https://youtu.be/dPfc2be8Ri8?si=R_bBk49ImOjPmcBw.
- **Open Data Portal:** https://youtu.be/OdZXI87VBn4?si=L11oFJg_aHcDqYTU.
- **Shared Technology Services:**
https://youtube.com/playlist?list=PL_QXqY3YNNV7OpzFrWCHCmSz5HRPm0Ibxp&si=XbO_ZKdq7LyhnXkAm.
- **Technology Guidance and Innovation:**
<https://youtu.be/p0NpHZkTtBY?si=lo00D66kDFsj4c3y>.
- **Technology Solutions Services:**
https://youtu.be/hYQ_M7cS6FQ?si=58VpqHVc_bQga0R.
- **Texas.gov:** <https://youtu.be/JyUGvihJVAc?si=YNQkVV8sEIljKXq>.
- **Texas by Texas:** <https://youtu.be/IOTfauf3pvY?si=6WuzPFEQzbJMiG9S>.

DIR Acronym List

ACH – Automated Clearing House

AI – Artificial Intelligence

AI-CoE – Artificial Intelligence Center of Excellence

AICPA – American Institute of Certified Public Accountants

AISAC – Automated Information Systems Advisory Council

AITC – Automated Information and Telecommunications Council

APM – Application Portfolio Management

APT – Advanced Persistent Threat

BELC – Business Executive Leadership Committee

BPR – Biennial Performance Report

CAC – Customer Advisory Committee

CAPPS – Centralized Accounting and Payroll/Personnel System

CCTS – Capitol Complex Telephone System

CDP – Closed Data Portal

CIO – Chief Information Officer

CIRT – Cybersecurity Incident Response Team

CIS – Center for Internet Security

CISA – Cybersecurity and Infrastructure Agency

CISO – Chief Information Security Officer

Cloud CoE – Cloud Center of Excellence

COOP – Cooperative Contracts Program

CPO – Chief Procurement Office

CRM – Customer Relationship Manager

CSA – Cloud Security Alliance

CSP – Cloud Service Provider

CTS – Communication Technology Services

CX – Customer Experience

CXO – Chief Experience Office

DCN – Data Center Network

DCS – Data Center Services

DDoS – Distributed Denial-of-Service

DHS – Department of Homeland Security

DMAC – Data Management Advisory Committee

DMO – Data Management Officer

DNS – Domain Name System

DPS – Department of Public Safety

EDR – Endpoint Detection and Response

EIR – Electronic and Information Resources

EIRAC – Electronic and Information Resources Accessibility Coordinator

ELT – Executive Leadership Team

EPEAT – Electronic Product Environmental Assessment Tool

ERCOT – Electric Reliability Council of Texas

ESF – Emergency Support Function

FedRAMP – Federal Risk and Authorization Management Program

FTE – Full-Time Equivalent

GAA – General Appropriations Act

GAATN – Greater Austin Area Telecommunications Network

GASB – Governmental Accounting Standards

GIS – Geographic Information System

GR – General Revenue

HB – House Bill

HCS – Hosted Collaboration System

HMSDC – Houston Minority Supplier Development Council

HR – Human Resources

HUB – Historically Underutilized Business

ILEAD – Innovative, Leadership, Ethical, Accountable, Delivery

IAM – Identity and Access Management

IBM – International Business Machines

IOC – Indicator of Compromise

IP – Internet Protocol

IR – Information Resources

IR-CAP – Information Resources Corrective Action Plan

IRDR – Information Resources Deployment Review

IRM – Information Resources Manager

ISF – Information Security Forum

ISO – Information Security Officer

IT – Information Technology

ITCHE – Information Technology Council for Higher Education

ITLC – Information Technology Leadership Committee

ITS – Information Technology Services

KPI – Key Performance Indicator

LAR – Legislative Appropriations Request

LBB – Legislative Budget Board

LMS – Legacy Modernization Strategy

MFA – Multi-Factor Authentication

MIRP – Major Information Resources Project

MOU – Memorandum of Understanding

MSI – Multi-Sourcing Services Integrator

MS-ISAC – Multi-State Information Sharing and Analysis Center

MSS – Managed Security Services

NASPO – National Association of State Procurement Officials

NCSR – Nationwide Cybersecurity Review

NIST – National Institute of Standards and Technology

NSOC – Network Security Operations Center

OAG – Office of Attorney General

OCDO – Office of the Chief Data Officer

OCISO – Office of the Chief Information Security Officer

ODP – Open Data Portal

ODPUG – Open Data Portal User Group

OGA – Operational Governance Authority

OGB – Operational Governance Board

OGC – Office of General Counsel

PBX – Private Branch Exchange

PCLS – Prioritized Cybersecurity and Legacy Systems

QAT – Quality Assurance Team

RAMP – Risk and Authorization Management Program

RSOC – Regional Security Operations Center

SaaS – Software as a Service

SAIC – Science Applications International Corporation

SB – Senate Bill

SCADA – Supervisory Control and Data Acquisition

SCP – Service Component Provider

SISAC – Statewide Information Security Advisory Committee

SOC – State Operations Center

SOW – Statement of Work

SPAR – Statewide Project Reporting Application

SPECTRIM – Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management

SSP – State Strategic Plan

STAR – Security, Trust and Assurance Registry

StateRAMP – State Risk and Authorization Management Program

STS – Shared Technology Services

TAC – Texas Administrative Code

TASSCC – Texas Association of State Systems for Computing and Communications

TCF – Texas Cybersecurity Framework

TDEM – Texas Division of Emergency Management

TDLP – Texas Data Literacy Program

TEA – Texas Education Agency

TEX-AN – Texas Agency Network

TMD – Texas Military Department

TSDEC – Texas Statewide Data Exchange Compact

TSS – Technology Solution Services

TxDOT – Texas Department of Transportation

TX-ISAO – Texas Information Sharing and Analysis Organization

TX-RAMP – Texas Risk and Authorization Management Program

TxT – Texas by Texas

URL – Uniform Resource Locator

VIRT – Volunteer Incident Response Team

VoIP – Voice over Internet Protocol

VSR – Vendor Sales Reporting

List of Figures

Figure 1 DIR's Strategic Vision	2
Figure 2 DIR Key Functions.....	4
Figure 3 Methods of Customer Feedback - Voice of the Customer.....	30
Figure 4 Organization Chart.....	107
Figure 5 FTE Caps for FY21 to FY25	108
Figure 6 Contracted Workforce by Quarter	108
Figure 7 Temporary or Contract Employees.....	109
Figure 8 Followers per Channel	119
Figure 9 2023 Phishing Campaign (January-June)	121
Figure 10 IT Support Tickets by Area FY22.....	121
Figure 11 DIR Turnover Rate.....	123
Figure 12 Red/Yellow/Green Health Indicator Metrics.....	124
Figure 13 DIR Projects Assigned a Project Manager in July 2023	124
Figure 14 DIR Board Member Onboarding Process	143
Figure 15 IT Operations' Ticket Intake Process.....	146
Figure 16 Process for the Initial Drafting of Documentation	146
Figure 17 Periodic Review and Updating of Business Process Documentation.....	147
Figure 18 CX Components Sequence.....	147
Figure 19 Method of Finance by Strategy	148
Figure 20 Auditors on Staff	152
Figure 21 TEX-AN Customers FY2022 by Channel and Billing.....	158
Figure 22 Work Order Process	164
Figure 23 Technician Process for Work Orders.....	165
Figure 24 Help Desk Workflow	166
Figure 25 Operator Call Intake Process	167
Figure 26 Total Logged Blocks by Month.....	180
Figure 27 Total Alert Notifications Sent to Agencies	181
Figure 28 Distributed Denial-of-Service (DDoS) Alerts.....	181
Figure 29 Priority I and Priority II DCS Security Incidents.....	182
Figure 30 July 2023 EDR Summary.....	182
Figure 31 EDR Count.....	183
Figure 32 Phishing Emails Analyzed per Month.....	184
Figure 33 Screen Capture of a Supervisory Control and Data Acquisition (SCADA) System	185
Figure 34 Vulnerabilities or System Compromises Chart	185
Figure 35 TX-ISAO Monthly Meeting Attendees	186
Figure 36 Security Bulletin Distribution	186
Figure 37 Functional Area Maturity 2014-2022.....	188
Figure 38 DIR-Funded Testing	188
Figure 39 TX-RAMP Assessments and Certifications.....	189
Figure 40 Cybersecurity Training and Compliance.....	189
Figure 41 July 2023 Phishing Simulation Results.....	190
Figure 42 InfoSec Academy Program Metrics.....	190

Figure 43 Organization Type Breakdown.....	191
Figure 44 Number of Training Programs DIR Certified	195
Figure 45 Eligibility Requirements for DIR Services	203
Figure 46 DIR Internet Gateway Architecture.....	206
Figure 47 NSOC Automated Intelligence Gathering.....	207
Figure 48 Four Teams within the Office of the Chief Information Officer	208
Figure 49 DIR's 2022 NCSR Self-Assessment Results.....	211
Figure 50 Workflow Process for CSP to Gain TX-RAMP Certification	216
Figure 51 VIRT Application Process.....	218
Figure 52 CIRT Incident Response Process.....	219
Figure 53 New Customer Onboarding Process	220
Figure 54 Onboarding Process for New TX-ISA0 Member	221
Figure 55 Workflow Process to Be Awarded a Texas Cyberstar Certificate	221
Figure 56 Workflow Process for Annual Security Awareness Training	222
Figure 57 DIR's 2022 NCSR Self-Assessment Results.....	235
Figure 58 OCDO Metrics	240
Figure 59 Open Data Portal Usage by Fiscal Year	241
Figure 60 Open Data Portal Onboard Process.....	248
Figure 61 Open Data Portal Posting Process.....	249
Figure 62 Cooperative Contract Sales (FY22)	263
Figure 63 Purchases and Savings by Customer Segment for FY21 and FY22.....	265
Figure 64 DIR HUB Outreach and Training Events	266
Figure 65 Cooperative Contracts Breakdown by Customer Type.....	268
Figure 66 Source Selection Authority.....	277
Figure 67 Method of Finance by Strategy	281
Figure 68 Data Center Services.....	291
Figure 69 Application Services Center	291
Figure 70 Service Delivery Model	292
Figure 71 STS Metrics.....	295
Figure 72 Service Level Agreements.....	295
Figure 73 Customer Satisfaction Monthly Scorecard	296
Figure 74 Overall STS Satisfaction	297
Figure 75 Overall Satisfaction Ratings-Historical.....	298
Figure 76 Responsibilities for Security in the Texas Public Cloud	300
Figure 77 Breakdown of Entities Affected	305
Figure 78 STS Governance Framework.....	308
Figure 79 FY22 Continuing Education Events.....	321
Figure 80 EIRAC Designation Compliance.....	322
Figure 81 Texas Agencies Digital Transformation Maturity	328
Figure 82 Planning and Reporting Framework.....	331
Figure 83 State Strategic Planning Process.....	332
Figure 84 Information Resources Deployment Review Process.....	332
Figure 85 Biennial Performance Reporting Requirements	333
Figure 86 Digital Transformation Process.....	336

Figure 87 Digital Transformation Tools	337
Figure 88 PCLS Workflow Process	338
Figure 89 Process to Create and Submit a PLCS Project.....	338
Figure 90 APM Agency Onboarding.....	339
Figure 91 LMS Engagement Process	340
Figure 92 AI-CoE Process	341
Figure 93 DIR Proof of Concept Lifecycle Methodology.....	341
Figure 94 State Strategic Plan Committee Requirements	343
Figure 95 Texas.gov Customer Satisfaction Monthly Scorecard	354
Figure 96 Texas.gov Performance Management Service Level Agreements.....	355
Figure 97 Types of Texas.gov Fees	362

List of Exhibits

Exhibit 1: Agency Contacts	1
Exhibit 2: Performance Measures – Fiscal Year 2022.....	37
Exhibit 3: Key Datasets	43
Exhibit 4: Policymaking Body.....	78
Exhibit 5: Subcommittees and Advisory Committees	87
Exhibit 6: Expenditures by Strategy – Fiscal Year 2022 (Actual)	104
Exhibit 7: Sources of Revenue – Fiscal Year 2022 (Actual).....	104
Exhibit 8: Federal Funds – Fiscal Year 2022 (Actual)	105
Exhibit 9: Fee Revenue – Fiscal Year 2022.....	105
Exhibit 10: FTEs by Location – Fiscal Year 2023	108
Exhibit 11: List of Program FTEs and Expenditures — Fiscal Year 2022	110
Exhibit 13: Statutes/Attorney General Opinions.....	367
Exhibit 14: 88 th Legislative Session	370
Exhibit 15: Contacts.....	395
Exhibit 16: Evaluation of Agency Reporting Requirements.....	402
Exhibit 17: Complaints Against the Agency (Vendor Protests) – Fiscal Years 2018-22	407
Exhibit 18: Purchases from HUBs	407
Exhibit 19: Equal Employment Opportunity Statistics.....	410

List of Supplemental Attachments

The following list of supplemental attachments is provided for review by the Sunset Advisory Commission. For security purposes, access to the supplemental attachments found in this list will be provided separately.

Attachment A: Organization Chart

Attachment B: Example Cybersecurity Operations Report sent to the Office of the Governor

Attachment C: DIR Branding and Style Guide

Attachment D: Chief Procurement Office Process Guide

Attachment E: Continuing Education Guide for State Agency Information Resources Managers

Attachment F: QAT Policies and Procedures Guide

Attachment G: FY22 Fee Schedule

Attachment H: 2022 Biennial Performance Report Telecommunications Performance