Sunset Advisory Commission

Staff Report

Department of Information Resources

2024-25
89th Legislature

Sunset Advisory Commission

Representative Justin Holland
Chair

To be appointed
Vice Chair

Representative Keith Bell
Representative Terry Canales
Representative Travis Clardy
Representative Matt Shaheen
Jeff Austin III, Public Member

Senator Angela Paxton
Senator Charles Schwertner, M.D.
Senator Drew Springer, Jr.
To be appointed
To be appointed, Public Member

Eric Beverly
Executive Director

Cover photo: The Texas State Capitol was completed in 1888. With the Goddess of Liberty atop the dome, the Texas State Capitol Building is 19 feet taller than the U.S. Capitol Building in Washington, D.C. The photo shows the south facade of the Capitol. Photo Credit: Janet Wood

Department of Information Resources

Sunset Staff Report

2024-25

89th Legislature

How to Read Sunset Reports

For each agency that undergoes a Sunset review, the Sunset Advisory Commission publishes three versions of its staff report on the agency. These three versions of the staff report result from the three stages of the Sunset process, explained in more detail at sunset.texas.gov/how-sunset-works. The current version of the Sunset staff report on this agency is noted below and can be found on the Sunset website at sunset.texas.gov.

CURRENT VERSION: Sunset Staff Report

The first version of the report, the Sunset Staff Report, contains Sunset staff's recommendations to the Sunset Commission on the need for, performance of, and improvements to the agency under review.

Sunset Staff Report with Commission Decisions

The second version of the report, the Sunset Staff Report with Commission Decisions, contains the original staff report as well as the commission's decisions on which statutory recommendations to propose to the Legislature and which management recommendations the agency should implement.

Sunset Staff Report with Final Results

The third and final version of the report, the Sunset Staff Report with Final Results, contains the original staff report, the Sunset Commission's decisions, and the Legislature's final actions on the proposed statutory recommendations.

Table of Contents

Summary of Sunset Staff Report

The Department of Information Resources (DIR) is in a much better position today than during its last Sunset review 12 years ago, when the agency was reeling from challenges with its beleaguered, consolidated data center services contract with IBM and its relationship with customers was universally abysmal. Since then, DIR has made significant improvements in its operations, including implementing contracting best practices and working hard to improve customer satisfaction.

As the state's information technology (IT) agency, DIR coordinates technology planning, oversees the state's cybersecurity posture, provides telecommunications services, and manages the state's cooperative IT procurements, data center, and state website. However, DIR is in a unique position. As a nonregulatory agency, DIR promotes best practices and sets statewide standards for data management and cybersecurity, but it has little authority to force agencies or other government entities to comply, even if enforcement would benefit Texans and better protect the state's information. Under the state's federated model, some government entities are required to use DIR's services, but otherwise they have significant control over their own IT. The Sunset review did not attempt to change this model and found DIR's current role in IT procurement and planning is appropriate, and that its division of responsibilities with other agencies is working well. Furthermore, the review did not attempt to fix all of the state's IT issues, many of which come down to limited funding. Instead, recommendations focus on addressing problems within DIR's existing framework, including improving opportunities for customer input and support to help ensure its customers get what they need and making sure DIR and the Legislature have the visibility needed to effectively plan for the state's future IT and cybersecurity needs.

DIR faces inherent challenges serving government entities of all sizes and with conflicting opinions.

As DIR outsources many of its functions, providing good customer service is integral to its success. Although the agency has made improvements, Sunset staff found better input mechanisms could help address the inherent challenges DIR faces serving government entities of all sizes, with sometimes conflicting opinions about IT needs. Throughout the review, Sunset staff heard a wide range of opinions about DIR and its services. Most customers expressed satisfaction with DIR's cooperative contracts, some praised DIR's data center services, and many were grateful for the agency's hands-on approach. On the other hand, several agencies wanted more autonomy from DIR on services like the public cloud and still lament the state's decision to have a consolidated data center. Other customers were frustrated by the difficulty in finding the right DIR contact to answer their questions or were confused about their eligibility for DIR's free or paid services. Recommendations to adjust DIR's advisory committees, restructure its board, and clarify communications around

eligibility would help alleviate this disconnect and promote better representation across the agency's current customer base.

Moreover, as DIR has generally improved its contracting processes and has had a role in overseeing major information resources projects almost since its inception, the review found DIR could do more to assist other agencies with their own IT procurements, given the risk to the state of those high-dollar contracts. Similarly, the review found a need for DIR to provide more training for staff of other agencies on best practices in IT contracting. While DIR's contracting program is generally well-run, the review also determined the agency could improve pricing controls for its Cooperative Contracts program (COOP) and reduce barriers requiring agencies to use sometimes more expensive staff augmentation services, in addition to strengthening its internal audit function. Addressing these issues will help ensure DIR can adequately provide assistance to other agencies on IT procurement.

Finally, given the Legislature's increased attention to and investment in cybersecurity over the last decade, DIR's role in overseeing the state's cybersecurity was a significant focal point for the review. Sunset staff focused on balancing DIR's nonregulatory role with a need to ensure the Legislature has accurate information to make decisions about IT funding and to protect the state's data. DIR and the Legislature have gaps in their overall picture of the state's cybersecurity posture that could be remedied by providing clearer information on cybersecurity and legacy systems' project funding needs and by requiring more frequent third-party assessments of agencies' cybersecurity.

The following material highlights Sunset staff's key recommendations for the Department of Information Resources.

Sunset Staff Issues and Recommendations

Issue 1

DIR's Customer Input Mechanisms and Board Structure Could Be Improved to Better Represent Its Customers and Help Ensure Their Needs Are Met.

Though DIR has improved customer input and satisfaction, some customers continue to have concerns with certain DIR programs. However, these concerns and suggestions differ widely and sometimes conflict due to differences in customer size and needs. To help address these differences in need, DIR could benefit from changes to its board structure to better reflect its primary customer base as well as changes to its advisory committee structure and customer feedback mechanisms to better solicit customer input to improve the agency's service delivery. DIR also could improve communication with existing and potential customers to reduce confusion surrounding customer eligibility, allowing more entities to take advantage of DIR's services.

Key Recommendations

- Restructure DIR's governing board to make all customer representatives nonvoting, ex officio members and expand the board to 11 members.
- Abolish two of DIR's expired statutory advisory committees, continue the Data Management Advisory Committee, and require DIR to establish certain advisory committees in rule.

- Direct DIR to improve communication to customers regarding eligibility and cost of services and create a formal process for potential customers to request eligibility.

Issue 2

DIR Could Improve Statewide IT Planning by Strengthening Its Reports to the Legislature and Expanding State Agency Procurement Support.

As the state's designated technology agency, DIR coordinates statewide IT planning and reporting by collecting state agency IT information and compiling reports for the Legislature. While DIR complies with statute when crafting these reports, the agency relies on entirely self-reported information from state agencies and has no process to verify this data, meaning the Legislature could be relying on reports based on incomplete or inaccurate information when making important policy decisions. DIR has the opportunity to strengthen these reports by strategically reviewing certain self-reported information and modifying its report on cybersecurity and legacy systems projects. Furthermore, as state agencies undertake increasingly expensive and risky IT projects, DIR is uniquely positioned to use its expertise in IT contracting to better train and assist staff of other agencies with their own IT procurements. Expanding DIR's IT procurement support would help agencies better plan, procure, and manage IT projects statewide.

Key Recommendations

- Require DIR to review a sample of IRDR responses for accuracy.
- Require DIR to develop an IT procurement certification and IT procurement training.
- Require DIR to develop a procurement-as-a-service pilot program.
- Direct DIR to clearly describe the risk associated with each quadrant in the *PCLS Report*.

Issue 3

Adjustments to Two of DIR's Main Contracting Programs Could Better Ensure the State Gets the Best Deal on IT.

DIR procures statewide contracts for information technology goods and services through COOP, Shared Technology Services (STS) contracts connected to the state's data center, and other outsourced programs. While DIR generally does a good job managing its contracted services and programs, the agency does not consistently ensure vendors post the list price for COOP products and services, which risks customers paying too much or unnecessarily moving on to a less suitable product or service. Additionally, providing DIR customers more flexibility in using funds appropriated for Data Center Services would allow them to choose the staff augmentation service that best suits their needs and budget and potentially save taxpayer dollars.

Key Recommendations

- The House Appropriations and Senate Finance committees should consider authorizing the use of Data Center Services funds for IT staff augmentation services through ITSAC.

- Direct DIR to review COOP vendor compliance at least twice per fiscal year to ensure pricing information is correct and posted timely.

Issue 4

DIR Needs More Tools to Protect the State's Cybersecurity.

Since the early 2000s, DIR has served an important role overseeing the state's cybersecurity, and this role grows ever more important as cybersecurity threats continue to evolve. DIR could further secure the state's cybersecurity by improving reporting to the Legislature on the state's cybersecurity posture and requiring state agencies to obtain certain third-party information security assessments periodically. DIR could also better leverage existing tools both to inform low-performing agencies and institutions of higher education of risks and remedies and to inform the Legislature of entities with the greatest needs. Finally, some statutory reporting requirements are redundant, creating confusion for agencies and institutions of higher education, and need to be consolidated.

Key Recommendations

- Require DIR to require state agencies under its jurisdiction to obtain a DIR-selected information security assessment periodically.
- Modify the existing *Information Security Assessment* reporting requirements to reduce redundancy.
- Direct DIR to change certain processes related to entities reporting low cybersecurity maturity.

Issue 5

The State Has a Continuing Need for the Department of Information Resources.

DIR has helped modernize connections between government entities and the Texans they serve. The agency enables government entities to harness the state's buying power, shared resources, and centralized IT procurement expertise to acquire and deploy the goods and services they need to best serve their constituents. DIR's coordination of IT and cybersecurity provides the state a more holistic picture of the systems currently used by government entities and the risks they pose, which helps the Legislature target funding and other improvements. No significant benefit would result from transferring functions or merging DIR with the state's other procurement or cybersecurity-related agencies. Additionally, a better documented risk assessment process with more input from board members would ensure DIR appropriately identifies the highest risks to the agency.

Key Recommendations

- Continue the Department of Information Resources for 12 years and remove the Sunset date of the agency's enabling statute.
- Direct DIR to document its ranking of risks identified in the audit plan and interview the board to inform the audit plan.

Fiscal Implication Summary

Though the recommendations in this report would not have a significant fiscal impact to the state, some recommendations could result in costs and savings that will depend on implementation and cannot be determined at this time. The cost of the recommendation in Issue 1 to expand the board to include one additional voting member would depend on whether the new member attends meetings virtually or in person, but DIR could absorb any minimal cost within its current budget. As a cost-recovery agency, DIR could offset the costs of recommendations in Issue 2 to develop and provide an IT procurement certification and to provide procurement-as-a-service through fees. DIR's implementation of these recommendations could contribute to cost savings from improved IT procurement across the state. In Issue 3, the recommendation for the House Appropriations and Senate Finance committees to consider authorizing the use of Data Center Services funds for IT staff augmentation services through ITSAC would not have a cost to the state as the recommendation does not contemplate appropriating additional funds for this purpose. This recommendation would allow DIR customers to choose the service that best suits their needs and budget. Other recommendations in the report would require DIR staff time to complete but could be implemented using existing resources.

Agency at a Glance

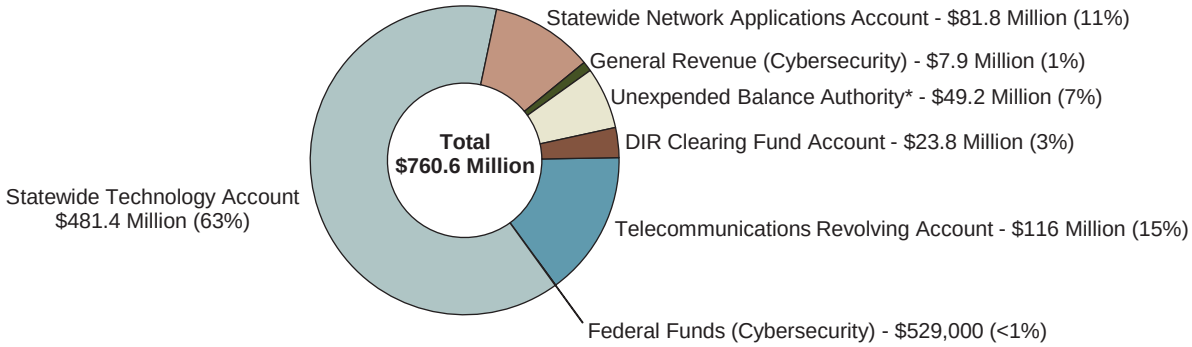
The Department of Information Resources (DIR) is the state's information technology (IT) and telecommunications agency. The Legislature created DIR in 1989 to coordinate the overall strategic direction for state agency use of IT, manage the state's computer services center, and approve information resources and telecommunications procurements.[1] As technology and state government have evolved in the last 35 years, DIR's responsibilities and its customer base have expanded significantly. Today, DIR procures and manages hundreds of IT contracts used by state agencies, institutions of higher education, school districts, and local governments throughout Texas as well as public entities in other states. Appendix A summarizes DIR's customers and available services. 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 achieve this mission, DIR carries out the following major functions:

- Provides guidance, planning, and reporting on statewide IT priorities for the Legislature and state agencies.
- Offers outsourced IT solutions and data management services to state agencies and other eligible public entities through the Shared Technology Services (STS) program.
- Procures IT products and services for eligible public entities through the Cooperative Contracts program (COOP).
- Provides telecommunications services to the Legislature and state agencies by operating the Capitol Complex Telephone System (CCTS) and through outsourced Texas Agency Network (TEX-AN) contracts.
- Establishes statewide cybersecurity and data management standards, supports governmental entities during cyberattacks, manages the state's Network Security Operations Center (NSOC), and oversees the state's data portals.

Key Facts

- **Governance.** DIR's 10-member board consists of seven governor-appointed, voting members and three nonvoting, ex officio members. The seven voting members serve staggered six-year terms, one of whom must be a member of an institution of higher education.[2] The three nonvoting, ex officio members serve two-year terms and rotate among two groups of agencies — the Texas Department of Insurance, Texas Health and Human Services Commission, and Texas Department of Transportation; and the Texas Department of Criminal Justice, Texas Parks and Wildlife Department, and Texas Education Agency.[3]
- **Funding.** In fiscal year 2023, DIR had $760.6 million in available revenue, as shown in the chart on the following page, *DIR Sources of Revenue*. DIR is a cost-recovery agency primarily funded by customer service fees, receiving $703 million in revenue across four cost-recovery accounts in fiscal year 2023. In fiscal year 2023, DIR also received $7.9 million in general revenue specifically allocated for cybersecurity. Additionally, DIR's sources of revenue include $49.2 million from fiscal year 2022 revenue that carried forward to fiscal year 2023.

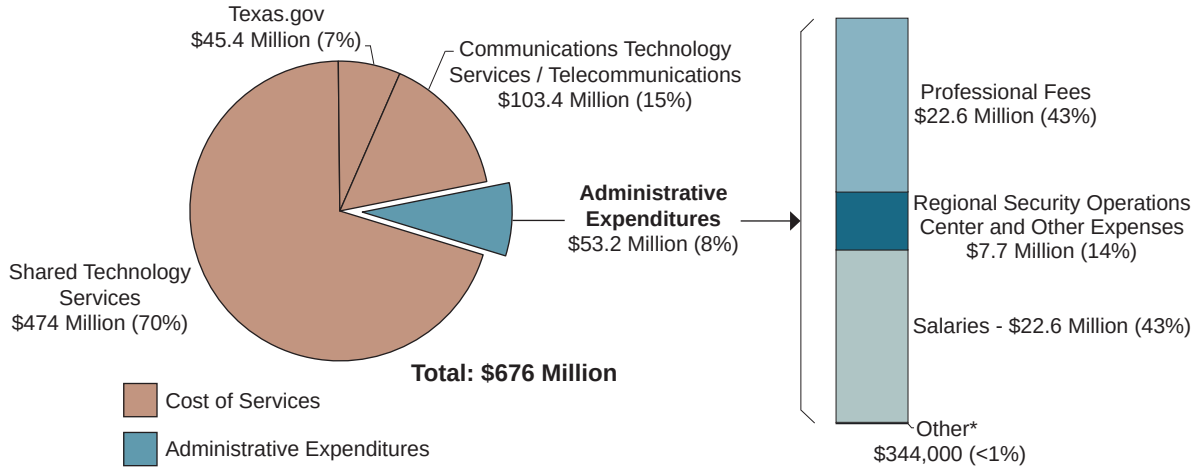
DIR Sources of Revenue - FY 2023



* Unexpended Balance Authority includes funds carried forward from fiscal year 2022.

As detailed in the *DIR Expenditures* chart, DIR's expenditures for fiscal year 2023 totaled approximately $676 million. Of this amount, 92 percent, or $622.8 million, represented cost of services payments to vendors for its major programs. DIR's administrative expenditures totaled $53.2 million, 43 percent of which went toward professional fees for education and training services, IT staff augmentation, market research, and cybersecurity testing. The $84.6 million difference between DIR's available revenue and expenditures was due to fund transfers and unexpended balance authority. In fiscal year 2023, DIR transferred $33.1 million in Texas.gov fees to the General Revenue Fund and approximately $9.7 million in other revenue to the Office of the Comptroller of Public Accounts. The agency also set aside $3.2 million for customer credits and rebates and set aside $38.5 million in unexpended balance authority to carry forward from fiscal year 2023 to fiscal year 2024. Appendix B describes the agency's use of historically underutilized businesses in purchasing goods and services for fiscal years 2021-23.

DIR Expenditures - FY 2023



* The Other category includes fuels and lubricants, consumables, utilities, travel, building rent, and machine rent.

- **Staffing.** In 2023, the Legislature increased DIR's employee cap from 228 to 267 for the 2024-25 biennium. Staff is located in Austin with the exception of one employee at the state data center in San Angelo. In addition to 221 agency staff, DIR works with 500 to 1,200 contractors at any given time to carry out the agency's main programs. DIR is home to four statutorily required statewide positions: the chief information officer of Texas, the chief data officer of Texas, the chief information security officer of Texas, and the state cybersecurity coordinator.[4] Appendix C compares the percentage of minorities and women in DIR's workforce to the statewide civilian labor force for the past three fiscal years.

- **IT planning and guidance.** DIR leads the state's strategic direction for IT development by publishing statewide IT priorities in the *State Strategic Plan for Information Resources Management*, reporting to the Legislature on agencies' technology and cybersecurity maturity, and providing guidance for major IT projects. DIR also coordinates outreach, training, and continuing education opportunities for 143 information resources managers at state agencies and provides IT contract and procurement training through the comptroller's office. Additionally, DIR staff serves on two statewide oversight committees, the Contract Advisory Team and Quality Assurance Team, which monitor major contracts and IT projects. To ensure government entities are keeping pace with the evolving technology sector, DIR manages emerging technology work groups, facilitates two Centers of Excellence for government cloud and artificial intelligence solutions, and supports the Artificial Intelligence Advisory Council.[5]

- **Shared Technology Services.** DIR offers outsourced IT solutions for public entities through four main STS programs: Data Center Services (DCS), Managed Security Services (MSS), Texas Open Data Portal, and the state's electronic platforms, which include Texas' official website and web and mobile application Texas.gov and TxT, respectively. The textbox below explains these components in greater detail. Appendix D depicts DIR's STS delivery model and lists all service categories available through the program.

Shared Technology Services

- **Data Center Services.** The DCS program operates two data centers, one located in San Angelo and the other in Austin, that provide mainframe computing and storage, public and private cloud management, application development, technology solution services, and print and digital document delivery. DIR delivers data center services to 115 public entities, including 25 designated state agencies required to participate and 90 voluntary customers.
- **Managed Security Services.** MSS provides cybersecurity services for public entities, including network monitoring and incident response. More entities use MSS than any other STS service, including all 254 Texas counties.
- **Texas.gov and TxT.** Texas.gov, the state's official website, and TxT, the state's official web and mobile application, provide secure platforms for Texans to conduct government transactions and find reliable state information. Texas.gov provides services for over 300 state agencies and local entities so constituents can complete license renewals, registrations, records requests, and more. Since TxT's launch in 2021, over 7 million people have created accounts, and Texas.gov processed nearly 60 million constituent transactions in fiscal year 2023.
- **Texas Open Data Portal.** The Open Data Portal is the state's central repository for publicly accessible data. State agencies use the portal to share data on various topics of public interest like agency complaints, license and permit datasets, and sales tax collections. Thirty-five state agencies posted 868 datasets on the portal by the fall of 2023. DIR also administers a Closed Data Portal to allow state agencies to share sensitive or confidential information in a secure environment with restricted access.

- **Cooperative Contracts.** DIR procures, negotiates, and manages approximately 800 contracts for discounted IT products and services through its COOP program. COOP operates under a self-service model, meaning public entities can purchase products as they need them, such as computer

hardware, software licenses, cloud storage, and IT staffing services — all with pre-negotiated terms and conditions that comply with state law. Statute requires state agencies to purchase IT commodities through COOP unless DIR approves an exemption, but other public entities, such as cities, counties, and school districts, can participate as well.[6]

- **Communications Technology Services.** DIR provides internet and telephone services for state agencies, the Legislature, local governments, institutions of higher education, and school districts. The agency directly operates CCTS and manages TEX-AN contracts, which provide outsourced options for voice and data services. Statute requires state agencies to use TEX-AN contracts for internet and phone service, but other eligible entities are voluntary customers.[7]

- **Cybersecurity.** DIR has provided network security services to state agencies since 2005. In 2017, the Legislature passed the Texas Cybersecurity Act and significantly expanded the agency's cybersecurity responsibilities.[8] Today, DIR protects state IT infrastructure by monitoring state agencies' internet traffic for malicious activity at the NSOC, establishing minimum cybersecurity standards, providing cybersecurity certifications and training, and offering cybersecurity products and services through the MSS program under STS. Additionally, DIR oversees security incident reporting and provides support for public entities during cybersecurity incidents, assisting with over 90 ransomware events since calendar year 2020. In 2022, DIR established a Regional Security Operations Center (RSOC) at Angelo State University, which trains university students for future cybersecurity roles and provides cybersecurity services to local governments, school districts, and institutions of higher education in West Texas. In 2023, DIR received appropriations to establish additional RSOCs at the University of Texas at Austin and the University of Texas Rio Grande Valley. DIR also leads the Texas Cybersecurity Council.

- **Data management.** DIR establishes statewide data guidance for public entities, provides free education and training through the Texas Data Literacy Program, and facilitates the Data Management Advisory Committee. As part of its role in statewide data management, DIR administers the Open Data Portal, Closed Data Portal, and the Texas Statewide Data Exchange Compact to facilitate state agency sharing of data.

---

1 Chapter 788 (HB 2736), Acts of the 71st Texas Legislature, Regular Session, 1989.

2 All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 2054.021(a) and (b), Texas Government Code.

3 Section 2054.021(c), Texas Government Code.

4 Sections 2054.0258, 2054.0286, 2054.510, and 2054.511, Texas Government Code.

5 Chapter 828 (HB 2060), Acts of the 88th Texas Legislature, Regular Session, 2023.

6 Section 2157.068(f), Texas Government Code; Chapter 242 (HB 4553), Acts of the 88th Texas Legislature, Regular Session, 2023.

7 Sections 2170.004 and 2170.051(c), Texas Government Code.

8 Chapter 683 (HB 8), Acts of the 85th Texas Legislature, Regular Session, 2017.

Issue 1

DIR's Customer Input Mechanisms and Board Structure Could Be Improved to Better Represent Its Customers and Help Ensure Their Needs Are Met.

Background

- **Board.** The Department of Information Resources (DIR) is governed by a 10-member board that sets the strategic direction for the agency, evaluates the agency's fulfillment of its mission, evaluates agency operations, and approves high-dollar contracts.[1] The board consists of seven governor-appointed voting members, one of whom must be from an institution of higher education (IHE), and three nonvoting, ex officio members representing state agencies.[2] Ex officio members rotate among two groups of agencies — the Texas Department of Insurance, Texas Health and Human Services Commission, and Texas Department of Transportation; and the Texas Department of Criminal Justice, Texas Parks and Wildlife Department, and Texas Education Agency.[3] DIR's current board is shown in the table below. Board members may not work for or have a substantial interest in a business in the information resources technologies industry that may contract with state government.[4]

DIR Governing Board

Name	Position	Voting Ability	Term Expires
Ben Gatzke, Board Chair	President and CEO, BorrowWorks, LLC	Voting	2029
Jeffrey W. Allison	Vice President of Business Development, Redtail Renewables	Voting	2028
Christopher "Stephen" Franke	Vice President, C1 Insurance Group	Voting	2028
Keith Halman	Associate Vice Chancellor and Chief Information Officer, Texas Tech University System	Voting	2030
Jeffrey Tayon	Independent Investor	Voting	2029
Vacant		Voting	
Vacant		Voting	
Cassie Brown	Commissioner of Insurance, Texas Department of Insurance	Nonvoting	2025
Anh Selissen	Chief Information Officer, Texas Department of Transportation	Nonvoting	2025
Maurice McCreary	Chief Operating Officer, Texas Health and Human Services Commission	Nonvoting	2025

The Legislature last substantially restructured the agency's board as part of its 1997 Sunset review.[5] At the time, the Legislature had made major changes to DIR's mission to remove its involvement in the review and approval of agencies' technology procurements and instead direct its focus on strategic planning of agency information resources, taking DIR's role from one of oversight to one of assisting state agencies.[6] This shift necessitated changing DIR's board to include state agency members to provide expertise and input. The agencies chosen as ex officio members were among the

state agencies with the largest number of employees and the most significant information resources expenditures, and they represented each of the major functions of state government.[7] Since 1997, the board's structure has not changed, with one exception in 2007 to replace the Texas Workforce Commission with the Texas Department of Insurance in the group of rotating agencies.[8] Institutions of higher education have had a voting seat on DIR's board since its creation in 1989.[9]

- **Advisory committees.** DIR has three statutorily required advisory committees, as described in the table below.[10] Statute also authorizes DIR to appoint advisory committees as necessary to provide expertise to the board and requires that at least one member of each advisory committee be an employee of a state agency.[11] In addition to the committees in statute, DIR established the Statewide Information Security Advisory Committee (SISAC) in 2011 to make recommendations to DIR for more effective information security operations.[12] DIR also has relationships with several statutory councils and uses other nonstatutory committees, councils, and groups, such as the Shared Technology Services (STS) governance groups described in Appendix E, to receive input and guidance on key programs.

DIR's Statutory Advisory Committees

Committee	Purpose	Membership	Statute
Customer Advisory Committee (CAC)	Reports to and advises the board on the status of DIR's delivery of critical statewide services, which could include services such as data center services, telecommunications, and the Texas.gov website.	Currently has 15 members. Customers who receive services from each of DIR's key programs, including state agencies with fewer than 100 employees and the public. To the extent practical, must represent a cross-section of DIR's customers.	Section 2054.0331, Texas Government Code
Data Management Advisory Committee (DMAC)	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; and establishes performance objectives for state agencies.	Currently has 106 members. DIR's chief data officer and each data management officer designated by a state agency and institution of higher education.	Section 2054.0332, Texas Government Code
State Strategic Plan for Information Resources Management Advisory Committee	Assists in the preparation of the *State Strategic Plan for Information Resources Management* that DIR's executive director is required to prepare for the board's review and approval.	Currently has 15 members. DIR rules require at least nine and no more than 21 members. Members appointed by DIR's executive director with the approval of the board. Must include at least two information resources managers, one higher education member, one public member, one local government member, three industry members, and one federal agency representative.	Section 2054.091(d), Texas Government Code

- **Customer eligibility.** The Legislature expanded DIR's customer eligibility in 2023 by authorizing DIR's executive director to determine that if participation in DIR services by certain entities, listed in Appendix A, is in the best interest of the state, those entities are eligible for services.[13] Prior to this change, many of these entities were eligible for some, but not all, of DIR's services.

Findings

DIR has made great strides since its last Sunset review in 2013 to improve customer input and satisfaction. Throughout this Sunset review, most DIR customers expressed general overall satisfaction with the agency's activities. However, Sunset staff also received considerable feedback that certain DIR programs need improvement, though these concerns and suggestions differed and sometimes conflicted due to differences in customer size and needs. Sunset staff focused on the structural aspects of customer input to relieve this disconnect and address changes in DIR's customer base. Representation needs have shifted over time, which has led to both over- and under-representation. The findings highlight a general need to update formalized approaches to soliciting input that will better represent DIR's main customers, increase transparency, fill in gaps in input, and foster discussions that can lead to better customer service over time.

Stakeholders indicate certain DIR programs need improvement, but concerns and suggestions differ.

DIR's board structure no longer reflects its primary customer base.

Sunset reviews consistently evaluate the structure of an agency's governing body to determine whether changes could improve responsiveness, accountability, or representation. Typically, the review must identify significant and systemic problems with an agency's operations to suggest measures as drastic as changing the existing governing structure. While Sunset staff's review of DIR did not reveal problems with board operations, DIR is relatively unique among agencies in that its primary customers are other state agencies and institutions of higher education as well as other public entities, rather than the broader public. As such, Sunset staff's evaluation considered whether the current board structure appropriately represents its main customer base and found that although state agency and higher education representation remains appropriate, some adjustments could improve the fairness and adequacy of that representation.

Adjustments to DIR's board could improve the fairness and adequacy of customer representation.

- **Outdated agency representation.** The group of agencies represented on DIR's board no longer reflects customers with the highest spending on DIR services, which are currently the Texas Health and Human Services Commission, Texas Department of Transportation, Office of the Attorney General of Texas, Texas Department of Public Safety, and Texas Department of State Health Services, only two of which are represented on the board. In addition, the current board membership is completely devoid of any small or midsize agencies, which often have differing information technology (IT) needs and challenges from the state's largest agencies. The DIR board could benefit from the expertise of its largest spending customers and small and midsize agencies to ensure the agency is responsive to their specific needs and provides services that are the best use of taxpayer dollars.

- **Outsized input.** IHEs maintain a unique role of authority in DIR's oversight. IHEs have a voting member on DIR's board, but state agencies do not despite the fact that state agencies, unlike IHEs, are required to use DIR

Certain agencies are required to use the state's data center, unlike institutions of higher education.

services in many instances.[14] For example, unlike IHEs, statute generally requires state agencies to use the Texas Agency Network (TEX-AN) for telecommunications services, the Capitol Complex Telephone System (CCTS) for telecommunications services within the capitol complex, DIR's Cooperative Contracts program (COOP) to procure most IT commodity items, and Texas.gov payment processing unless DIR grants a state agency an exemption.[15] Certain state agencies are also required to use the state's data center, while institutions of higher education are not.[16] In addition, state agencies are often top spenders across DIR programs. For the STS, Texas.gov, and CCTS programs, state agencies were the top five spenders in each category in fiscal year 2023. For the COOP program, in fiscal year 2023, state agencies spent over 88 percent more than IHEs, with state agencies spending $968.7 million versus IHEs spending $514.1 million. Appendix A shows the DIR programs that statute requires state agencies to use, unlike IHEs which are voluntary customers.[17] In addition, since IHEs are the only voting customer group on DIR's board, they have an outsized influence on DIR's decision making in comparison to state agency customers. For example, the IHE voting member on the board votes to approve DIR's major contracts that state agencies are often required to use, but state agencies do not have the same power in decision making.[18]

IHEs have another formal mechanism to provide important input to DIR on issues that affect them. The statutory Information Technology Council for Higher Education (ITCHE) consists of the chief information officers or equivalent employees from the major public university systems in the state.[19] Statute requires DIR to prepare, in consultation with ITCHE, an analysis of the impact of proposed DIR rules that apply to IHEs but does not require this of any other customer group, including state agencies.[20] Statute requires DIR to include the analysis as part of the notice of the proposed rule that DIR files with the secretary of state for publication in the *Texas Register* and requires DIR to provide a copy of this analysis to the governor, lieutenant governor, and speaker of the House of Representatives.[21]

DIR's advisory committee structure could better solicit feedback from customers to improve the agency's service delivery.

Under the Sunset Act, an agency's advisory committees are abolished on the same day as the agency unless expressly continued by law, but continuing the agency does not automatically continue its advisory committees by extension.[22] Additionally, other law provides that a statutory advisory committee expires four years after the date it was established unless either: (1) statute exempts the advisory committee from that provision, or (2) the agency sets a later date for expiration in rule.[23] Agencies may also have authority to create in rule advisory committees, some of which may be subject to the same four-year limitation. As a result, Sunset must sometimes determine whether an advisory committee should be continued.

- **The Customer Advisory Committee has expired by operation of law and does not function as intended.** In its current form, CAC does not serve the purpose for which the Legislature created it and because DIR's rules governing the committee do not include an expiration date, the committee has been expired by operation of law since 2017.[24] The Legislature, through the Sunset process, established CAC in 2013 at a time of extreme customer dissatisfaction with DIR.[25] Statute requires the committee to report to and advise the board on the status of the agency's delivery of critical statewide services.[26] However, CAC is not currently operating as a true advisory committee. In practice, DIR primarily presents information on a particular topic instead of the committee members driving the conversation and providing input and advice to DIR, as an advisory committee typically does. In the last several years, a CAC member has only formally presented to the board once, and the committee has never provided any specific recommendations for the board's consideration.

  CAC has never provided any specific recommendations for the board's consideration.

  Although the committee no longer keeps meeting minutes, based on incomplete minutes from 2018 to 2020 and Sunset staff's observations, CAC meetings are not well attended. With such a broad mission, fostering meaningful input from and discussion among committee members can be challenging because members may only use certain DIR programs, leaving them struggling to find common ground. By comparison, DIR's STS governance groups, such as the IT Leadership Committee, are guided by a formal agenda sent to participants prior to the meeting, are well attended, and foster robust discussion between committee members and DIR staff.

- **The State Strategic Plan for Information Resources Management Advisory Committee has expired by operation of law but serves a valuable function.** DIR's rules do not provide an expiration date for the State Strategic Plan for Information Resources Management Advisory Committee and as a result, the committee is expired by operation of law.[27] Though the committee has expired, the need for stakeholder input into DIR's state IT planning remains critical to ensure all stakeholders, such as state agencies, IHEs, the public, local government, and the IT industry, have an opportunity to provide input on issues that affect them. Including stakeholders in state IT planning brings a wide range of expertise to the process and ensures DIR can better plan for the future of IT in the state.

  Stakeholder input into DIR's state IT planning remains critical.

- **The Statewide Information Security Advisory Committee functions well but is not defined in rule.** Using its statutory authority to establish advisory committees, DIR created SISAC in 2011.[28] The committee is comprised of information security professionals from state and local government and aims to share ideas and best practices among its members and make recommendations to DIR for more effective information security operations. Though SISAC serves an important function, it has operated for over a decade without the agency establishing the committee in rule or defining its purpose or duration in rule, as required by statute. General law requires agencies to establish in rule the purpose and tasks of its

advisory committees and to describe the manner in which the committee will report to the agency.[29]

- **DIR continues to need the Data Management Advisory Committee.** DMAC is relatively new, as the Legislature created it in 2021 as part of a larger effort to help agencies improve their data management and governance.[30] DMAC is exempt from the four-year statutory limitation, and it continues to serve an important function because improving agencies' data management practices is still a work in progress.[31]

- **DIR could benefit from filling gaps in customer input on COOP and from small and midsize agencies.** DIR has no formal mechanism to receive customer input on COOP, meaning DIR may not be aware of or understand the extent of common problems customers have with a vendor or contract. DIR also lacks input on whether COOP customers are getting the products and services they want. In fiscal year 2023, nearly $3.4 billion in public funds from 3,400 entities ran through COOP, which statute generally requires state agencies to use.[32] Throughout the review, Sunset staff heard from stakeholders who were very satisfied with COOP, but some expressed frustration and confusion with DIR's COOP website, the breadth of contracts offered, and the timeliness for vendors to be added to COOP as a reseller, or they indicated they could receive better prices for IT goods and services on the open market. With a formal customer input mechanism, DIR could receive information on these issues and address problems with COOP in an organized, rather than ad hoc, manner.

DIR struggles to receive input from small and midsize state agencies.

DIR also struggles to receive input from small and midsize state agencies, which often have limited resources and bandwidth to focus on IT and could benefit from more assistance from DIR, as discussed further in Issue 2. However, DIR does not have a formal way for small and midsize agencies to provide input to the board on their specific needs. While large agencies often have significant IT, data management, and cybersecurity staff in-house, small or midsize agencies may have very few staff filling all of these roles in addition to other responsibilities, or they may rely on contracted staff. Small and midsize agencies still have substantial IT needs, and the databases they operate can still involve significant personally identifiable information and large amounts of data, meaning they rely greatly on IT solutions provided by DIR.

DIR does not post basic information about some advisory committees on its website.

- **DIR's advisory committees could be more transparent.** DIR does not post any information about CAC on its website. DIR does include basic information about SISAC and DMAC, such as the committees' general goals. However, the agency makes no information on meeting dates, agendas, materials, minutes, recordings, or committee membership available for any of its statutory advisory committees.[33] Without this basic information, customers may not be aware of established avenues to provide input and may lack information about programs that affect them.

Improved communication could reduce confusion regarding customer eligibility, allowing more entities to take advantage of DIR's services.

Under DIR's expanded customer eligibility, every entity listed in Appendix A is potentially eligible for all of its programs, subject to DIR approval. However, the agency does not clearly indicate in which circumstances it would typically approve or deny use of its services. In addition, DIR has not made a process clear for entities to request eligibility under its newly expanded eligibility allowance, meaning entities wishing to use DIR services may not know how to access them.

DIR's webpage lacks important detail.

DIR did not update its customer eligibility webpage to its current version to reflect its expanded eligibility until Sunset staff inquired about it. Nevertheless, the webpage lacks important detail, such as which entities are eligible for free versus paid services, meaning potential customers could be missing out on cost-effective contracts and cybersecurity services that are increasingly vital as public entities across the state rely on technology and face cyberattacks.[34] For example, DIR does not clearly communicate that it offers network penetration tests for free to state agencies, IHEs, and public junior colleges, but local governments and independent school districts have to pay for this service. River authorities also can benefit from free services but may not know they exist because, though provided in DIR's *Security Services Guide*, this information is not clear on DIR's website.[35]

Further confirming these concerns, in a Sunset staff survey of local governments and school districts, 116 out of 364 respondents indicated they were unfamiliar with DIR. Sunset's conversations with other stakeholders and reviews of river authorities have consistently proven some entities have little to no idea they are eligible for certain DIR services; river authorities are often unaware of DIR's free cybersecurity services, and school districts are usually familiar with COOP but not with DIR's other programs.

DIR does not have a formalized way to measure customer satisfaction with its telecommunications services, meaning the Legislature may not be receiving accurate information.

DIR's results from its telecommunications survey may be misleading.

The Legislative Budget Board (LBB) tracks two key performance measures to monitor customer satisfaction with DIR's telecommunications programs, but DIR's results may be misleading. DIR reports the results of two customer satisfaction surveys in accordance with these performance measures.[36] The surveys are supposed to be available online, but in practice DIR only includes survey links at the bottom of telecommunications staff email signatures. In fiscal year 2023, this survey method yielded just 45 responses for the CCTS survey and 37 responses for the TEX-AN survey, out of DIR's over 900 telecommunications customers. Any individual who receives an email from telecommunications staff can fill out the survey, which may lead to flawed data due to an unrepresentative sample, the lack of targeted survey recipients, and haphazard survey distribution. With insufficient customer surveys, DIR

and the Legislature have a limited view into telecommunications customers' experience and needs.

DIR's statutes do not reflect standard language typically applied across the board (ATB) during Sunset reviews.

The Sunset Commission has developed a set of standard recommendations that it applies to all state agencies reviewed unless an overwhelming reason exists not to do so. These ATBs reflect an effort by the Legislature to enact policy directives to prevent problems from occurring, instead of reacting to problems after the fact. ATBs are statutory administrative policies adopted by the Sunset Commission that contain "good government" standards. The ATBs reflect review criteria contained in the Sunset Act designed to ensure open, responsive, and effective government.

A recent SAO audit found DIR's board members had not completed contract training.

- **Board training.** DIR's statute contains standard language requiring board members to receive training and information necessary for them to properly discharge their duties. However, statute does not require the agency to create a training manual for all board members or specify that board members must attest to receiving and reviewing the training manual annually.[37] Additionally, a recent State Auditor's Office audit found DIR's board members had not complied with another requirement in statute to complete contract training, which is important given the board's oversight of DIR's extensive contracting.[38] Sufficient training ensures board members are adequately equipped to carry out their duties.

- **Missing complaint form.** DIR's statute contains language requiring the agency to maintain detailed complaint information. However, instead of requiring DIR to make information available describing its complaint procedures generally, statute only requires DIR to provide that information to individuals involved in a complaint.[39] DIR provides an "Ask DIR" submission box on its website for general input, but the website lacks a clear complaints form with instructions and information about the complaint process. While DIR does not receive many complaints, it should still maintain a complaints form to help ensure it addresses documented problems in a timely fashion.

Sunset Staff Recommendations

Change in Statute

1.1 Restructure DIR's governing board to make all customer representatives nonvoting, ex officio members and expand the board to 11 members.

This recommendation would restructure DIR's governing board to better reflect its current customer base and expand the size of the board to 11 members to ensure an odd number of voting members, as depicted in the table on the following page. Under this recommendation, the three rotating, ex officio state agency representatives would be replaced with one member from a state agency with fewer than 500 full-time equivalent employees and two members from a list of the 10 state agency customers with the highest levels of spending on DIR products and services in the previous fiscal year. DIR would provide a

list of the state agencies with the highest spending levels to the governor biennially. Nonvoting members would rotate out at the end of their term with the governor choosing replacements. This recommendation would also change the higher education member from a voting to nonvoting board member and align their term length with the other nonvoting members to two years. IHEs would still have ITCHE as an avenue for formal analysis of the impact that DIR's proposed rules have on higher education.

All members would be appointed by the governor with voting members also receiving Senate confirmation. Existing board members would continue to serve the remainder of their terms and would be replaced by the governor at the end of their terms. Changing the structure of the board in this way would ensure fair representation of customers and allow DIR's largest customers and small to midsize agencies with different needs to have a voice on the board. This recommendation does not include nonvoting members from local governments and school districts because these entities are not required users of DIR services.

Proposed New Board Structure

Number	Voting Ability	Appointment and Position	Term
7	Voting members	Governor appointed with Senate confirmation.	Six-year term
2	Nonvoting members	Governor appointed. Must be an employee of a state agency among the 10 largest DIR customers.	Two-year term
1	Nonvoting member	Governor appointed. Must be an employee of a state agency with fewer than 500 full-time equivalent employees.	Two-year term
1	Nonvoting member	Governor appointed. Must be an employee of an institution of higher education as defined by Section 61.003, Texas Education Code.	Two-year term

1.2 Abolish two of DIR's expired statutory advisory committees and require DIR to establish certain advisory committees in rule.

This recommendation would remove the CAC and State Strategic Plan for Information Resources Management Advisory Committee from statute since both have expired by operation of law. In place of these statutory advisory committees, this recommendation would modify DIR's existing statutory authority to appoint advisory committees to require DIR to establish advisory committees in rule for the following core functions, at a minimum: COOP, information security, and *State Strategic Plan for Information Resources Management*. This recommendation would also require DIR to create a customer advisory committee composed of state agencies with 500 or fewer full-time equivalent employees, including at least three members from a state agency with 150 or fewer full-time equivalent employees, to ensure DIR receives input from these underrepresented groups.

As part of this recommendation, DIR would be required to establish SISAC in rule. This recommendation would not require DIR to establish its STS governance model in rule because they are not technically advisory committees and do not report to DIR's board. However, this recommendation would encourage the agency to use an STS advisory committee or add additional members to its existing groups to seek input from more non-designated customers and small to midsize agencies to better understand how it can improve services for those groups.

The recommendation would require all advisory committees other than DMAC and other committees already exempted in statute be subject to Chapter 2110, Texas Government Code. In addition to the existing statutory requirement that all DIR advisory committees include a member from a state agency, all advisory committees established in rule using DIR's general authority would be required to include at

least one member from a state agency with 500 or fewer full-time equivalent employees. In considering membership for these committees, DIR should, to the extent practicable, ensure representation from a cross-section of customers that use the related DIR service.

The department would be required to adopt rules regarding each advisory committee, including but not limited to:

- The purpose, role, goals, and duration of the committees.
- Appointment procedures, composition, terms, and quorum requirements.
- Qualifications of the members, as necessary.
- Training requirements, if needed.
- Conflict-of-interest policies.
- The method the agency will use to receive public input on issues considered by the advisory committees, as appropriate.
- The method for sharing committee information with the public and DIR's board, as appropriate.

DIR should examine all of its programs to evaluate whether an advisory committee for the program would improve the department's operations and stakeholder input. As a management action, DIR should provide comprehensive information on its website related to its advisory committees to improve transparency of DIR's customer input processes.

1.3 Continue the Data Management Advisory Committee.

This recommendation would continue DMAC, which is active and continues to serve an ongoing need.

1.4 Update the standard across-the-board requirement related to board member training.

This recommendation would require the agency to develop a training manual that each board member attests to receiving annually and require existing board member training to include information about the scope of and limitations on the board's rulemaking authority. The training should provide clarity that the Legislature sets policy and that agency boards and commissions have rulemaking authority necessary to implement legislative policy. The recommendation also would require board members to attest to completing all required training, including contract training, before voting.

1.5 Update the standard across-the-board requirement related to developing and maintaining a complaints system and making information on complaint procedures available to the public.

This recommendation would update the statutory language requiring DIR to develop and maintain a complaints system and make information on complaint procedures available to the public.

Management Action

1.6 Direct DIR to improve communication to customers regarding eligibility and cost of services.

Under this recommendation, DIR would post to its website in a clear and consistent manner information for each customer group detailing eligibility for an available service and whether a service is free or provided at a cost. DIR could also consider creating a communications plan to reach out to entities unfamiliar with DIR, which could include presenting at conferences attended by representatives from river authorities, school districts, and other local government entities who are unfamiliar with DIR's services but could benefit from using them.

1.7 Direct DIR to create and communicate a formal process for a potential customer to request customer eligibility from DIR's executive director.

Under this recommendation, DIR would create a form on its website for an entity to request eligibility for DIR's services. DIR would clearly communicate which entities must fill out the form to be considered for eligibility by service type. Providing such a form would clearly communicate that entities may request to use DIR's services but would not require DIR to approve that request. DIR should publish a list of entities approved for services to its website. As DIR makes decisions approving some entities and not others for its services, providing more information up front would save both DIR staff and entities considering using DIR services time and effort.

1.8 Direct DIR to formalize annual telecommunications customer service surveys for the CCTS and TEX-AN programs.

Currently, DIR has online survey tools and maintains CCTS and TEX-AN customer listservs. Using this existing toolset, DIR should deploy an annual survey of CCTS and TEX-AN customers to gather feedback from all telecommunications customers and make the survey open over a fixed, rather than rolling, timeline. DIR could consider using other formalized customer service surveys, such as the monthly STS surveys, as a model for its telecommunications survey. Deploying the survey to all CCTS and TEX-AN customers over a standard timeframe would provide the Legislature and LBB more meaningful information with which to evaluate DIR's performance and would allow DIR to better understand CCTS and TEX-AN customer experiences and make informed decisions about future telecommunications procurements.

Fiscal Implication

Recommendation 1.1 to expand the board could be accomplished with existing resources. While DIR reimburses board members for travel expenses, the cost would depend on whether new board members attended meetings and trainings virtually or in person, and DIR could absorb any minimal cost within its current budget. Recommendation 1.6 to improve communication with customers would have no cost to the state because DIR already posts some customer eligibility information to its website, and further website updates could be accomplished with existing staff. If DIR chooses to develop and implement a communications plan as part of Recommendation 1.6, the cost to the state would depend on implementation, such as additional statewide travel, and cannot be determined at this time. All other recommendations could be implemented using existing resources.

[1] 1 Texas Administrative Code (TAC), Part 10, Chapter 201, Section 201.4 (e-g) (2022) (DIR, *Board Policies*); 1 TAC, Part 10, Chapter 201, Section 201.6(d) (2017) (DIR, *Contract Approval Authority and Responsibilities*).

[2] All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 2054.021, Texas Government Code.

[3] Ibid.

[4] Section 2054.022(a), Texas Government Code.

[5] Chapter 606 (SB 365), Acts of the 75th Texas Legislature, Regular Session, 1997.

[6] Texas Sunset Advisory Commission (SAC), *Texas Department of Information Resources Staff Report*, January 1996, pp. 35-40, accessed online March 13, 2024, https://www.sunset.texas.gov/public/uploads/files/reports/Department%20of%20Information%20Resources%20Staff%20Report%201996%2075th%20Leg.pdf.

[7] Ibid., p. 40.

[8] Chapter 9 (HB 675), Acts of the 80th Texas Legislature, Regular Session, 2007.

[9] Chapter 788 (HB 2736), Acts of the 71st Texas Legislature, Regular Session, 1989.

[10] Sections 2054.0331, 2054.0332, and 2054.091, Texas Government Code.

[11] Section 2054.033, Texas Government Code.

[12] DIR, *Statewide Information Security Advisory Committee (SISAC)*, accessed online March 13, 2024, https://dir.texas.gov/information-security/security-policy-and-planning/statewide-information-security-advisory-committee.

[13] Chapter 242 (HB 4553), Acts of the 88th Texas Legislature, Regular Session, 2023.

[14] Chapter 788 (HB 2736), Acts of the 71st Texas Legislature, Regular Session, 1989.

[15] Sections 2054.382, 2170.051(c), 2157.068, and 2054.113, Texas Government Code.

[16] Section 2054.382, Texas Government Code.

[17] Sections 2054.003(13) and 2057.068, Texas Government Code.

[18] Section 2054.382, Texas Government Code.

[19] Section 2054.121, Texas Government Code.

[20] Section 2054.121(c), Texas Government Code.

[21] Section 2054.121(d), Texas Government Code.

[22] Section 325.013, Texas Government Code.

[23] Section 2110.008, Texas Government Code.

[24] 1 TAC, Part 10, Chapter 201, Section 201.5 (2014) (DIR, *Advisory Committees*).

[25] Chapter 48 (HB 2472), Acts of the 83rd Texas Legislature, Regular Session, 2013; SAC, *Texas Department of Information Resources Final Report with Legislative Action*, July 2013, p. 15, accessed online March 13, 2024, https://www.sunset.texas.gov/public/uploads/files/reports/DIR%20and%20Procurement%20Staff%20Report%202013%2083rd%20Leg.pdf.

[26] Section 2054.0331(d), Texas Government Code.

[27] 1 TAC, Section 201.5.

[28] Section 2054.033, Texas Government Code; DIR, *Statewide Information Security Advisory Committee (SISAC)*, accessed online March 13, 2024, https://dir.texas.gov/information-security/security-policy-and-planning/statewide-information-security-advisory-committee.

[29] Section 2110.005, Texas Government Code.

[30] Chapter 567 (SB 475), Acts of the 87th Texas Legislature, Regular Session, 2021.

[31] Section 2054.0332(d), Texas Government Code.

[32] DIR, *Self-Evaluation Report*, August 2023, pp. 268-269, accessed online March 16, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf; Section 2157.068, Texas Government Code.

[33] DIR, *Statewide Information Security Advisory Committee (SISAC)*, accessed online March 16, 2024, https://dir.texas.gov/information-security/security-policy-and-planning/statewide-information-security-advisory-committee; DIR, *Information for Data Officers*, accessed online March 16, 2024, https://dir.texas.gov/office-chief-data-officer/information-data-officers.

[34] DIR, *Customer Eligibility*, accessed online March 13, 2024, https://dir.texas.gov/it-solutions-and-services/customer-eligibility.

[35] DIR Office of the Chief Information Security Officer, *Security Services Guide*, Version 1.2, April 2023, p. 2, accessed online April 15, 2024, https://dir.texas.gov/sites/default/files/2024-01/2024%20DIR%20OCISO%20Security%20Services%20Guide.pdf.

[36] DIR, Article I, page I-80, Chapter 1170 (HB 1), Acts of the 88th Legislature, Regular Session, 2023 (General Appropriations Act).

[37] Section 2054.021, Texas Government Code.

[38] SAO, "An Audit Report on a Selected Contract at the Department of Information Resources", May 2021, pp. 16-18, accessed online April 26, 2024, https://sao.texas.gov/Reports/Main/21-018.pdf.

[39] Section 2054.036, Texas Government Code.

Issue 2

DIR Could Improve Statewide IT Planning by Strengthening Its Reports to the Legislature and Expanding State Agency Procurement Support.

Background

As the state's designated technology agency, statute requires the Department of Information Resources (DIR) to coordinate statewide information technology (IT) planning and reporting.[1] To fulfill this requirement, DIR collects IT information from state agencies and uses it to compile reports for the Legislature. DIR relies on designated staff at each state agency, called information resources managers (IRMs), to fill out required IT surveys.[2] Every biennium, DIR conducts two critical surveys — the Information Resources Deployment Review (IRDR), which is required for state agencies, and the Prioritized Cybersecurity and Legacy Systems (PCLS) questionnaire, which is voluntary.[3]

As described in the *IRDR Components* textbox, the IRDR is a comprehensive survey about an agency's IT environment, standards compliance, alignment with state technology goals, and IT inventory.[4] DIR aggregates IRDR responses and then publishes the *Biennial Performance Report on the Use of Information Resources Technologies by Texas State Agencies (BPR)*, which details state agency progress on IT goals, describes major IT issues facing agencies, and makes recommendations to the Legislature related to technology.[5] In addition to the *BPR*, DIR uses agency IRDR responses to inform several other statutorily required reports, including the *PCLS Report*, as described in the textbox on the following page.[6] The *PCLS Report* ranks state agency cybersecurity and legacy projects in order of priority for funding.[7]

IRDR Components

Statute requires state agencies to submit the following information, which DIR gathers through the IRDR:

- **Agency environment** — a summary of information security, digital accessibility, continuity of operations, project management, data management, and privacy practices.
- **Compliance with state standards** — confirmation by the agency of compliance with state statutes, rules, and standards relating to information resources. If a state agency is out of compliance, it must submit an information resources corrective action plan (IR-CAP).
- **Alignment with state technology goals** — an analysis of an agency's alignment with the progress and goals in the *State Strategic Plan for Information Resources Management*.
- **IT inventory** — a listing of an agency's major information systems (such as servers or cloud services), major databases, applications, and telecommunications network configuration.

DIR Reports Using IRDR Information

- *Biennial Performance Report on the Use of Information Resources Technologies by Texas State Agencies*
- *Biennial Cybersecurity Report*
- *Prioritized Cybersecurity and Legacy Systems Report*
- *Biennial Consolidated Assessment of Agency IT Infrastructure Report*
- *Biennial Electronic Information Resources Accessibility Report*
- *Biennial Report on Project Management Practices*
- *Biennial Report on Internet-Based Training*

While DIR manages the IRDR process, it is not the only entity authorized to view agencies' IRDR responses. Statute also requires state agencies to submit IRDR responses to the Quality Assurance Team (QAT), which includes one representative each from DIR, the Legislative Budget Board (LBB), State Auditor's Office (SAO), and Office of the Comptroller of Public Accounts.[8] QAT provides oversight for major IT projects that have significant impact on the state or cost $5 million or more.[9] As part of this oversight, statute requires QAT to monitor the life cycle of each major IT project — including its schedule, cost, scope, and quality — and publish an annual report for state leadership on IT project management trends.[10] QAT also reviews contracts for IT projects that cost $10 million or more.[11] To identify major IT projects for monitoring, QAT members may consult the IRDR responses agencies submit.

Findings

DIR's mechanisms to help the Legislature plan for and prioritize IT and cybersecurity projects need improvements to ensure more accurate and complete information for decision making.

DIR relies on self-reported information from state agencies for its statutorily required reports to the Legislature, including the *BPR*, *Biennial Cybersecurity Report*, and *PCLS Report*. Collectively, these reports provide state leadership with vital insight into state agency IT compliance, tools, and needs and have the potential to inform IT policy and funding decisions.[12] Ensuring all reports are clear, complete, and accurate is critical for the state's cybersecurity and IT planning.

DIR lacks a mechanism to verify agencies' self-reported information.

- **Unverified IRDR responses.** DIR receives important information from state agencies in the IRDR, but this data is fully self-reported and DIR lacks a mechanism to verify information agencies report. While Sunset staff did not identify incorrect IRDR responses, no tool exists to check the information. Incorrect data in the IRDR could result in a ripple effect of the Legislature getting inaccurate information in all the legislative reports the IRDR feeds into. For example, the IRDR is a major reporting vehicle for several statutorily required reports on digital accessibility requirements, project management, internet-based training, IT infrastructure, and standards compliance, and the Legislature uses information in these reports to make decisions about the future of IT. If agencies provide incorrect information, DIR and the Legislature may not be able to identify gaps in the state's IT infrastructure and address them in a timely manner, meaning the state may miss out on opportunities to stay on top of IT innovation.

  DIR also uses IRDR data to answer questions from the Legislature and inform interim committees' work. For example, the Legislature created the

Texas Work Group on Blockchain Matters in 2021 to study the growing blockchain industry in Texas and make legislative recommendations for this emerging field.[13] At the work group's request, DIR used IRDR responses to provide background information on state agency IT systems and cybersecurity insurance for the members, providing important context for its policy recommendations. The work group's final report listed 21 legislative recommendations that impacted various sectors, including energy, finance, and state government.[14] If IRDR responses are inaccurate, DIR and the Legislature could develop unsuitable policies for emerging technologies that do not reflect state agency realities and needs.

- **Unclear *PCLS Report* risk categories.** While the current iteration of the *PCLS Report* meets the statutory requirement to provide a prioritized list of cybersecurity and IT modernization projects, the descriptions of the projects' risks in the report are technical and difficult to understand.[15] When DIR published the first *PCLS Report* in 2016, it contained information from 82 projects that totaled $379 million. In comparison, the *2022 PCLS Report* contained 95 projects totaling $927 million. As funding amounts balloon and cybersecurity risk increases, the Legislature needs reliable and clear information about which projects are highest priority, most impactful, and most deserving of funding, and unclear information unnecessarily complicates the Legislature's funding decisions.

  In addition to ranking all projects, to depict a project's risk in the *PCLS Report*, DIR places each project in a quadrant. DIR uses statistical methods to put projects in four quadrants, each representing a level of priority and risk. However, neither the confidential nor public version of the report explains how DIR calculated which projects should be in which quadrant. Additionally, neither version of the report describes each quadrant's risk in layman's terms. For example, quadrant I projects pose great risk to a state agency's cybersecurity or operations and need to be funded this biennium, compared to quadrant IV projects which are less urgent, but this is not explicitly stated in the report. Furthermore, DIR does not indicate how quickly the Legislature should consider funding a project in quadrant II or how different the cybersecurity risks are between quadrants II and III, even though legislators and LBB staff need this level of detail to decide which projects need immediate funding and which can be funded over multiple biennia.

The Legislature needs clear information about which IT and cybersecurity projects are highest priority.

The state's IT procurement support could be improved, delivering cost savings and efficient government services to Texans.

Public entities of all sizes struggle with IT project delivery, and DIR is uniquely qualified to improve IT procurements statewide. However, it needs to expand its current trainings and services to do so.

- **Agencies struggle with increasingly expensive and risky IT procurements.** Texans increasingly expect government services to be available online,

The majority of recent large IT projects were behind schedule or over budget.

and state agencies are modernizing to meet constituent needs, often with multiple high-dollar IT procurements. However, QAT has historically found common problems with state agency planning of IT procurements, and Sunset reviews have found agencies of all sizes struggle with IT procurement, as detailed in the textbox below.[16] According to QAT, the majority of large IT projects in the 2023 annual report were behind schedule or over budget, delaying government services and costing the state money.[17] In this same report, QAT found only 15 out of 50 IT projects over $5 million were within 10 percent of their originally planned duration and budget.[18] Once major IT projects are completed, state agencies must submit post-implementation reviews that describe project obstacles and lessons learned. In 2023, QAT reported that 63 percent of post-implementation reviews identified project planning — including the project's original scope and schedule — as a major cause of delays and overspend.[19] Adequately planned IT procurements are more likely to be on time and on budget, avoiding these problems altogether.

Complicated IT Procurements at State Agencies

- **Teacher Retirement System of Texas (TRS) IT System.** A 2020 Sunset review found TRS experienced dozens of issues with its large contract for a new IT system. TRS amended the contract 45 times and ultimately terminated the contract when it was over schedule by 50 percent, over the initial contract value, and with only one phase of the contract completed. TRS ultimately assumed two major project components in-house due to vendor performance limitations.
- **Texas Commission on Law Enforcement (TCOLE) Database.** A 2020 Sunset review found TCOLE's IT contracting processes were underdeveloped; staff were not adequately trained on procurement, and TCOLE did not conduct robust risk assessments or design contracts with sufficient reporting and performance incentives to hold the vendor accountable for problems. As a result, the vendor continued to be paid under the contract though it was unable to meet deadlines for deliverables and provide a fully functioning database on schedule, keeping TCOLE operating on an outdated database.
- **Texas Department of Licensing and Regulation (TDLR) Licensing System.** A 2020 Sunset review found TDLR lacked a cohesive approach to collecting and reporting inspection data and recommended that TDLR implement data-driven strategies with the new licensing system being procured. Prior to the Sunset review, TDLR began its effort to modernize and consolidate its nine legacy licensing systems into one, requesting $1.95 million in the 2020-21 biennium for phase one of the project. In 2022-23, TDLR requested and the Legislature appropriated $2 million for phase two of the project. However, TDLR encountered vendor delays and lost confidence, deciding not to renew the contract and returned appropriated funds. Following this unsuccessful effort, TDLR developed a project plan and requested $32.9 million in fiscal years 2024-25 for the licensing system, a significant sum.
- **Texas Board of Veterinary Medical Examiners (TBVME) Database.** A 2022 Sunset review found TBVME's poor contracting practices significantly delayed the agency's efforts to upgrade its licensing and enforcement database. TBVME contracted with vendors for a database in 2018 and 2020. The agency spent at least $183,000 on database vendors, but both procurements failed. In the most recent biennium, the Legislature temporarily attached TBVME to TDLR, appropriated $1.2 million to TBVME to procure a database, and mandated the agency work with DIR on this procurement.

- **DIR has extensive IT and procurement experience.** No other state agency has comparable experience with IT procurement and contract management, making DIR an excellent resource for agencies struggling with IT projects. Currently, DIR procures and manages about 800 cooperative contracts,

11 Shared Technology Services contracts, and 22 Texas Agency Network (TEX-AN) telecommunications contracts, with a cumulative value of over $4.4 billion over the length of the contracts.[20] In addition to its own procurements, statute tasks DIR with providing contract training to state agencies, and DIR also provides support and consultation for state agencies upon request. For example, DIR frequently works with agencies to transfer their databases and important applications to the state's data center, and when needed, to define statements of work for DIR's cooperative contracts. DIR also hosted one-on-one workshops with the Texas Department of Insurance and the Public Utility Commission of Texas to explore various IT solutions for modernization.

Furthermore, DIR has improved its contracting practices since previous Sunset reviews. Sunset identified only minor contracting concerns in this review, as discussed in Issue 3, and SAO has not had any priority findings for DIR on contracting since 2020.[21] In SAO's annual contract monitoring report for large agencies, DIR was rated as "no additional monitoring warranted" for all contracting periods in 2022.[22]

DIR has improved its contracting practices since previous Sunset reviews.

- **State agencies could benefit from additional IT contract training.** Statute requires DIR to provide IT procurement and contract training through several avenues, as described in the accompanying textbox.[23] Though DIR is following statute and supporting procurement staff and executive leadership where it can, the agency could do more. Throughout the Sunset review, stakeholders expressed a need for increased training and clarity on IT procurement processes. Several state agency respondents to a Sunset staff survey of DIR customers requested more training on IT contracting, noting that technology projects can be more complicated and expensive than other procurements. While current state certifications for contract developers and DIR trainings equip staff with general procurement knowledge, they do not provide in-depth and specialized training needed to successfully manage complex technology procurements. For example, DIR's portion of the CTCD certification training addresses how to procure IT products and services through DIR but does not provide specifics on how to avoid common problems with complex IT procurements in general such as properly defining scope, remedies, and addressing vendor turnover. This level of detail is especially important for major information resources projects over $5 million that could take several years to implement. For small agencies in particular, IT projects can be several times their biennial information resources budget, increasing the need for properly trained staff. For example, the State Pension Review Board has a small budget and received $600,000 for the creation of a new interface and self-service

Procurement and Contract Training

- **QAT annual training.** As a QAT member, DIR provides annual training on best practices for IT contracts required by statute.
- **IT contract negotiations training.** Statute requires DIR to provide a training on IT negotiations for all state employees involved in IT negotiations. DIR provides a one-hour "IT Negotiations" webinar and an "Advanced IT Negotiations" webinar.
- **Certified Texas Contract Developer (CTCD) training.** DIR's portion of the CTCD certification is about two hours and covers DIR services and IT procurement basics.
- **Certified Texas Contract Manager (CTCM) training.** DIR's portion of the CTCD certification is one hour and focuses on IT purchasing basics and DIR services.

reporting portal.[24] Additionally, none of the procurement and contract trainings specifically target agency executive staff despite the fact they play a critical role in IT modernization initiatives through strategic planning and budgeting and could benefit from basic information on IT procurement to help their staff avoid common pitfalls.

Sunset Staff Recommendations

Change in Statute

2.1 Require DIR to review a sample of IRDR responses for accuracy.

Under this recommendation, DIR would select a sample of at least five IRDR responses for review and verify the accuracy on a biennial basis. DIR would not review all sections of the IRDR in the selected sample. Instead, DIR should consider which questions have the highest-impact data and information regarding agency software, hardware, compliance, and cybersecurity. To select which agency responses to review, DIR could consider risk factors such as IRM participation in continuing education, history of compliance with information resources statute and rule, and any anomalies in IRDR submission such as missing answers or inconsistencies with the previous year's data. DIR would conduct a desk review of the responses and should use the results to inform future trainings and outreach to IRMs on how to accurately complete the IRDR and to direct agencies toward IT solutions as needed. Results of the review could also help agencies identify potential funding needs and serve as a tool in their legislative appropriations requests. Ultimately, state agency IRDR responses are the foundational documents of the state's IT policy, and verifying this data would promote accuracy and completeness as the Legislature makes important statewide IT policy decisions.

2.2 Require DIR to develop an IT procurement certification.

Under this recommendation, DIR would develop an in-person IT procurement certification course and offer it on a quarterly basis for certified Texas contract developers (CTCDs) and certified Texas contract managers (CTCMs), and those with dual certification. While available to all CTCDs and CTCMs, participation in the IT procurement certification would be voluntary. DIR could consider modeling the course on the Technology Procurement Specialization Certificate available through the National Institute of Governmental Purchasing. In developing the certification, DIR should ensure the completed course would qualify for continuing education hours for the CTCD, CTCM, or dual certifications available through the comptroller's office.

2.3 Require DIR to develop an IT procurement training for state agency executive leadership.

Under this recommendation, DIR would develop a high-level training on IT procurement for state agency executives and offer it on at least an annual basis. While available to all state agency executives, participation in the training would be voluntary. DIR should ensure the training includes information on relevant topics DIR already provides training on through its portion of the CTCD and CTCM trainings, as well as additional topics at DIR's discretion. Dedicated IT procurement and contract training for executive staff would equip them with the knowledge they need to assist their staff in procuring and managing successful IT projects that improve government services for Texans.

2.4 Require DIR to develop a procurement-as-a-service pilot program.

Under this recommendation, DIR would pilot a program to assist state agencies with IT procurement upon request, until January 1, 2029. DIR would have discretion to approve agency participation in the pilot as well as the number of participants and type of projects allowed in the pilot program. DIR's assistance under the pilot could include, but would not be limited to, helping agencies with procurement planning, developing a cost estimate for a potential IT project, and drafting and developing a solicitation. The agency requesting assistance would have full legal control and liability for the project, and the agency would manage the contract until the project's completion. Once completed, DIR would report to the Legislature by December 1, 2028, summarizing the status of the pilot and providing a determination of whether the Legislature should continue or expand the pilot. Providing procurement-as-a-service would improve agency IT projects statewide, save tax dollars, and improve the modernization of state IT.

Management Action

2.5 Direct DIR to clearly describe the risk associated with each quadrant in the *PCLS Report*.

Under this recommendation, DIR would provide a plain language description in the *PCLS Report* of the methodology used to place projects into quadrants. The description should include, at a minimum, an explanation of the risk associated with each quadrant using simple-to-understand terms and which quadrant includes projects that could be broken into multiple phases or funded across biennia. Providing this information would allow LBB and appropriators to have clear information with which to make decisions.

Fiscal Implication

Overall, these recommendations would not have a significant fiscal impact to the state. Recommendations to review IRDR responses, modify the *PCLS Report*, and provide high-level procurement training to agency executive staff could be accomplished with existing resources. DIR has staff dedicated to assisting with the IRDR and already provides in-depth assistance to help agencies complete it properly, and Recommendation 2.1 would require DIR to review a limited number of responses and only portions of the IRDR for accuracy. Furthermore, when the Legislature created the IRDR, no significant fiscal implication was anticipated for agencies to provide the information, suggesting costs to DIR to verify that information should also not be significant.[25] For Recommendation 2.2, DIR could recover the cost of one additional staff needed to develop and provide the IT procurement certification through certification fees charged to agencies receiving the training. While the total cost to participants for the certification cannot be determined at this time since the course would be voluntary, DIR estimates the course would cost approximately $475 per person, similar to the cost for contract certifications through the comptroller's office, and the cost to agencies would depend on the number of employees taking the course. For Recommendation 2.4, costs for DIR to provide procurement-as-a-service could be offset by fees customers pay for DIR's services. The cost to agencies requesting the service cannot be determined at this time as it would be determined by DIR. Overall, implementing these recommendations would contribute to improved IT reporting and cost savings from improved IT procurement across the state.

---

[1] All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Sections 2054.051, 2054.052, and 2054.091, Texas Government Code.

[2] Section 2054.074, Texas Government Code.

[3] Sections 2054.069(b) and 2054.0965, Texas Government Code.

[4] Sections 2054.464, 2054.055(b)(8)-(11), 2054.068, 2054.157(b), 2054.515, 2054.0965(b)(5), 2054.0965(b)(6), 2054.0965(b)(4), 2054.0965(b)(1)-(b)(3), and 2054.069, Texas Government Code.

[5] Section 2054.055, Texas Government Code.

[6] Sections 2054.055, 2054.0591, 2054.069, 2054.068, 2054.068, 2054.055(b)(9), 2054.157(b), and 2054.055(b)(8), Texas Government Code.

[7] Section 2054.069, Texas Government Code.

[8] Sections 2054.097 and 2054.158, Texas Government Code.

[9] Sections 2054.003(10) and 2054.160, Texas Government Code.

[10] Section 2054.159, Texas Government Code.

[11] Section 2054.158(4), Texas Government Code.

[12] DIR, *Information Resources Deployment Review Instructions*, last updated March 13, 2024, p. 4, accessed online March 13, 2024, https://dir.texas.gov/sites/default/files/2024-01/2024%20IRDR%20Instructions.pdf.

[13] Chapter 320 (HB 1576), Acts of the 87th Texas Legislature, Regular Session, 2021.

[14] Texas Work Group on Blockchain Matters, *A Report to the Members of the Texas Legislature*, November 2022, p. 6-8, accessed online April 1, 2024, https://data.texas.gov/w/qzgk-h93r/7v57-4sdh?cur=hqnlC4TaHf7.

[15] Section 2054.069, Texas Government Code.

[16] Texas Sunset Advisory Commission (SAC), *Teacher Retirement System of Texas Staff Report*, April 2020, pp. 19-21, accessed online March 27, 2024, https://www.sunset.texas.gov/public/uploads/files/reports/TRS%20Staff%20Report%20with%20Final%20Results_6-30-21.pdf; SAC, *Texas Commission on Law Enforcement Staff Report*, November 2020, pp. 21-23, accessed online March 27, 2024, https://www.sunset.texas.gov/public/uploads/files/reports/TCOLE%20Staff%20Report%20with%20Final%20Results_6-30-21.pdf; SAC, *Texas Department of Licensing and Regulation Staff Report*, June 2020, pp. 81-84, accessed online March 27, 2024, https://www.sunset.texas.gov/public/uploads/files/reports/Texas%20Department%20of%20Licensing%20and%20Regulation%20Staff%20Report%20with%20Final%20Results_6-30-21.pdf.; Invited testimony before the Investment in Information Technology Improvement Joint Oversight Committee, Austin, August 30, 2022; SAC, *State Board of Veterinary Medical Examiners Special Purpose Review Staff Report*, June 2023, pp. A1, 5-6, accessed online March 27, 2024, https://www.sunset.texas.gov/public/uploads/2023-08/State%20Board%20of%20Veterinary%20Medical%20Examiners%20Special-Purpose%20Review%20with%20Final%20Results_6-26-23.pdf.

[17] Quality Assurance Team, *Annual Report: Overview of Major Information Resources Projects Reported to the Quality Assurance Team December 2022 to November 2023*, December 2023, pp. 1-2, accessed online February 19, 2024, https://qat.dir.texas.gov/2023QATAnnualReport.pdf.

[18] Ibid., p. 1.

[19] Ibid., p. 5.

[20] DIR, *Self-Evaluation Report*, August 2023, pp. 105, 156, 294, and 312, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[21] State Auditor's Office (SAO), *An Audit Report on Financial Processes at the Department of Information Resources*, April 2020, p. ii, accessed online March 23, 2024, https://sao.texas.gov/reports/main/20-029.pdf.

[22] SAO, *A Report on Contract Monitoring Assessment at Certain State Agencies*, April 2022, p. 5, accessed online March 23, 2024, https://sao.texas.gov/Reports/Main/22-027.pdf.

[23] Sections 2054.158(b)(3), 656.050, and 656.052, Texas Government Code; 34 Texas Administrative Code (TAC), Part 1, Chapter 20, Subchapter B, Section 20.133(2022)(Office of the Comptroller of Public Accounts, *Training and Certification Program*).

[24] Chapter 995 (HB 2), Acts of the 87th Texas Legislature, Regular Session, 2021.

[25] Chapter 691 (HB 1788), Acts of the 80th Texas Legislature, Regular Session, 2007.

Issue 3

Adjustments to Two of DIR's Main Contracting Programs Could Better Ensure the State Gets the Best Deal on IT.

Background

The Department of Information Resources (DIR) procures statewide contracts for information technology (IT) goods and services through its Cooperative Contracts program (COOP), telecommunications services through the Texas Agency Network (TEX-AN), and Shared Technology Services (STS) contracts connected to the state's data center. The table below shows DIR's main contracted functions, number of contracts, contract value, number of customers, and fees DIR charged on each contract for fiscal year 2023.[1]

DIR Contracts - FY 2023

Program	Contracts	Contract Value	Customers	DIR Fee
Cooperative Contracts (COOP)	800	$3.4 billion in total sales	3,400	0.5-1%
Shared Technology Services (STS, not including Texas.gov)	9	$3.6 billion	796	2.95%
Texas.gov	2	$600 million	89	0-3.0%
TEX-AN	22	$110 million	4,000	0.5-12%

- **COOP.** Through COOP, DIR competitively procures zero dollar, master contracts with hundreds of vendors for IT goods and services, and negotiates standard terms and conditions as well as minimum discounts. COOP is a self-service model that allows DIR's customers, such as state agencies, local governments, school districts, and other states, to buy products and services to implement on their own. When customers buy through COOP, the final contract is between the vendor and the customer. COOP vendors offer products and services either through a prime contract in which a vendor sells products directly, or as a subcontractor under the prime contract that either sells its own products and services or resells other manufacturers' products.

  DIR requires all COOP vendors to post up-to-date pricing information through a link on the COOP website, including the manufacturer's suggested retail price (MSRP) if applicable and the discount DIR negotiated. DIR's website provides a direct link to the vendor's website with prices and discount information to avoid frequently amending the contract if the price changes. The discount varies based on the type of product or service. For most products, DIR does not negotiate a certain price for a product, only a discount percentage off MSRP.

- **STS.** Under the STS program, DIR procures and manages contracts with vendors to offer eligible customers services, including public and private cloud solutions, mainframe, application development and maintenance, managed security services, and digital commerce such as electronic payments through the Texas.gov website. STS contracts are between DIR and the vendor. Appendix D shows STS services in more detail.

- **IT staff augmentation.** IT Staff Augmentation Contracts (ITSAC) provide temporary IT staff to eligible COOP customers on an as-needed hourly basis. Staff augmentation experience levels range

from interns to highly experienced and specialized IT staff. Technology Solution Services (TSS), under the STS umbrella, also offers staff augmentation services through the TSS Rate Card program to Data Center Services customers.

Findings

Pricing information is inconsistently available for COOP contracts, increasing the risk DIR's customers are overpaying for IT products and services.

DIR does not consistently ensure vendors post the MSRP for COOP products and services, which risks customers paying too much or unnecessarily moving on to a less suitable product or service. When DIR's customers are comparing COOP products, the lack of available price lists also increases the administrative burden on them to contact the vendor or contract manager for updated pricing when that burden should be on DIR. Customers need to see the MSRP to know if the vendor has inflated its price in violation of DIR's agreement and, if the customer is not required to use COOP, to verify that DIR's discounted price is competitive. During the review, Sunset staff found four examples of COOP contracts with missing price information, as summarized in the accompanying table. While DIR conducts website checks when renewing or amending COOP contracts, which can happen as infrequently as every two years, it does not conduct more frequent spot checks to ensure vendors keep the MSRPs posted and up to date.

COOP Contracts Missing MSRP

Product or Service	Reason for Missing MSRP
Servers, software, and storage	Staff turnover at vendor and file was corrupted.
Information security services	Unpredictable nature of the kind of services requested.
Software as a service	No reason.
Software through a reseller	No reason.

In addition, inaccurate price lists can result in COOP customers overpaying or wasting taxpayer funds even after they enter into a contract for a product or service. A fiscal year 2023 internal audit of a $39 million contract with Xerox found the vendor had, through a keystroke error, entered incorrect prices for certain items on its master price list, resulting in customers paying more than the contractually agreed-upon price. The overcharge in this case was small, but small errors across DIR's 800 COOP contracts and thousands of products and services under those contracts could result in the state wasting money.

Sunset staff found four examples of COOP contracts with missing price information.

Unnecessary barriers prevent DIR customers from using less expensive staff augmentation contracts, resulting in the state potentially spending more than it needs to on IT staff.

ITSAC, under COOP, and TSS Rate Card, under the STS program, both offer staff augmentation services to DIR customers. However, the prices are not always comparable, and some DIR customers are locked into using a potentially more expensive TSS staffing option because funds appropriated for Data Center Services may only be spent on STS programs, of which TSS is one. The textbox on the following page shows a comparison of TSS hourly rates that are consistently higher than the lowest level ITSAC rates, not including the even lower intern-level ITSAC rates.[2] ITSAC rates vary depending on

levels of staff expertise while each staff position through TSS has a single rate that increases each fiscal year. Although TSS can be a more cost-effective option in some cases and includes more concierge-type assistance with IT projects than ITSAC, if customers need only entry-level staff, they cannot use their Data Center Services funds to obtain the less expensive staff through ITSAC. This restriction results in the state sometimes paying more for staffing than it needs to, risking wasting taxpayer dollars.

Examples of Lower ITSAC Hourly Rates Compared to TSS - FY 2024

Data Analyst
ITSAC: $54.87 level one to $147.25 level three
TSS Rate Card: $105.47

Data Engineer
ITSAC: $87.30 level one to $142.24 level three
TSS Rate Card: $111.02

Data Scientist
ITSAC: $87.30 level one to $142.24 level three
TSS Rate Card: $116.57

Web Software Developer
ITSAC: $50.91 level one to $123.38 level three
TSS Rate Card: $94.37

In addition to occasionally higher hourly rates, the TSS option may be even more expensive because of DIR's higher administrative fee for STS. DIR applies and collects a higher fee of 2.75 percent for fiscal year 2024 from customers using the STS program, including TSS, while the administrative fee for ITSAC under COOP is 1 percent for fiscal year 2024.[3] Furthermore, using the more expensive staffing option through TSS can be unnecessary after a customer implements a TSS project, because maintaining a project, such as a database or website, may not require the same level of expertise as building it, and ITSAC offers more flexibility in both pricing and levels of expertise.

Sunset Staff Recommendations

Change in Appropriation

3.1 The House Appropriations and Senate Finance committees should consider authorizing the use of Data Center Services funds for IT staff augmentation services through ITSAC.

This recommendation would express the will of the Sunset Commission that the Legislature consider authorizing funds appropriated for Data Center Services to be used on staff augmentation services offered through ITSAC in addition to services offered through TSS Rate Card. For example, the Legislature could consider allowing agencies to transfer funds out of Data Center Services for ITSAC purposes with automatic Legislative Budget Board approval after 30 days, contingent on agencies documenting associated cost savings. Removing the current restriction would allow DIR customers to choose the staff augmentation service that best suits their needs and budget — either ITSAC or TSS.

Management Action

3.2 Direct DIR to review COOP vendor compliance at least twice per fiscal year to ensure pricing information is correct and posted timely.

Under this recommendation, DIR would conduct a risk-based assessment of vendor compliance with existing requirements to post correct pricing information on the COOP website. DIR could consider assessing risk based on the total value of the contract, contracts with the most customers, contracts with

the most subcontractors, vendors that had not previously held a COOP contract, or other criteria the agency identifies. As part of the risk-based assessment, DIR should choose a representative sample of COOP contracts to check for violations of the service level agreement to post updated pricing information. DIR should conduct risk-based website compliance checks at least twice per fiscal year and may stagger checks on groups of vendors throughout the fiscal year. More frequent reviews of vendor compliance would help ensure customers can easily compare the prices of products and services on COOP.

Fiscal Implication

Overall, these recommendations could be accomplished with existing resources and would not have a fiscal impact to DIR or the state. Recommendation 3.1 would allow DIR customers receiving legislative appropriations to use funds designated for Data Center Services on ITSAC vendors but would not appropriate additional funds for this purpose. While Recommendation 3.2 would require additional effort from DIR, verifying vendor compliance with contract terms is part of the agency's contract oversight responsibilities and could be accomplished with existing resources. Both recommendations would help ensure the state does not overspend on IT products and services.

---

1 All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 2157.068, Texas Government Code establishes DIR's statutory authority to set administrative fees. For Texas.gov, in addition to the percentage fee, DIR charges fees for each transaction that vary depending on the services each customer negotiated. The number of contracts and customers for COOP is approximate, as it fluctuates throughout the year.

2 ITSAC levels correspond to staff years of experience, with level one meaning one to three years of experience in a given field, level two meaning four to seven years, and level three meaning over eight years. Rates reflect the maximum price that may be billed. Customers may negotiate lower rates.

3 In fiscal year 2024, DIR reduced the STS fee from 2.95 percent to 2.75 percent.

Issue 4 | DIR Needs More Tools to Protect the State's Cybersecurity.

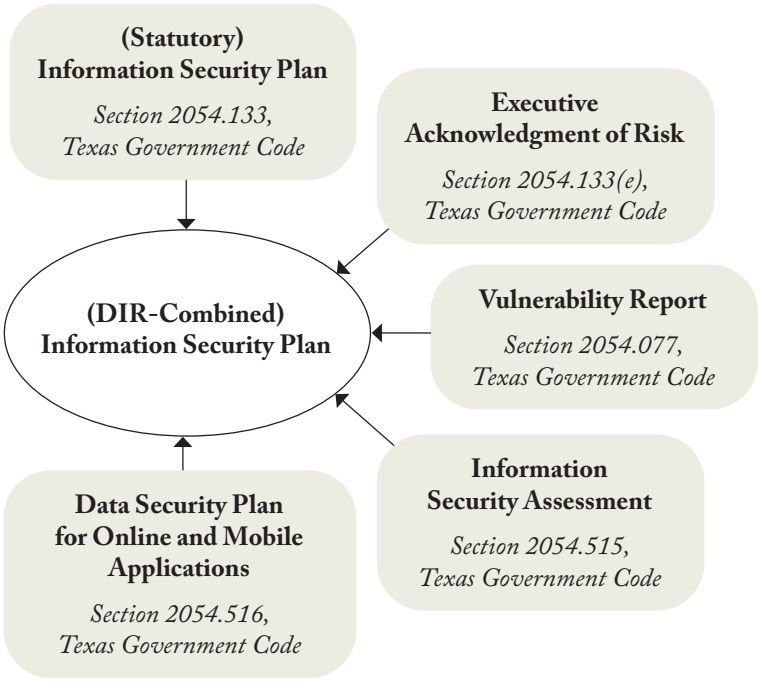
Background

The Legislature first charged the Department of Information Resources (DIR) with cybersecurity in the early 2000s when it mandated that the agency develop a statewide cybersecurity program and established DIR's duty to protect the state network.[1] Since Sunset's previous review in 2013, DIR's role in cybersecurity has increased significantly, as depicted in Appendix F. Today, statute requires DIR to set rules creating and governing minimum standards that entities — meaning state agencies and institutions of higher education, including community colleges — must adhere to in their cybersecurity practices.[2]

The primary tool DIR uses to evaluate entities' cybersecurity development is called the Texas Cybersecurity Framework (TCF), which grades entities' maturity in terms of how well they identify, protect against, detect, respond to, and recover from cybersecurity threats.[3] DIR designed this tool in response to the Legislature passing Senate Bill 1134 in 2013 and based the TCF on existing standards from the National Institute of Standards and Technology (NIST), which is a highly technical federal agency responsible for "advancing measurement science, standards, and technology."[4]

Statute requires each entity to complete multiple biennial reporting requirements and submit responses to DIR detailing aspects of the entity's cybersecurity. The rectangles in the graphic to the right show the individual reports that entities must send to DIR. DIR refers to these requirements collectively as the *Information Security Plan*, represented by the oval in the accompanying graphic, since DIR requires entities to use the statutory *Information Security Plan's* reporting tool to submit information for all reporting requirements. The table on the following page provides greater detail on each individual requirement.

***Information Security Plan* Components**



Information Security Plan Components

Component	What DIR Requires Entities to Submit
Information Security Plan, also known as the "Biennial Self-Assessment" and the "Agency Security Plan"	• Self-assessment of cybersecurity maturity against around 40 standards outlined in the TCF. • Includes a roadmap of future actions and roadblocks for each standard.
Information Security Assessment	• In practice, the assessment includes the same information required for the *Information Security Plan*. • Self-assessment of the information security of the entity's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities. • Also includes a requirement for a data governance assessment, which entities report separately from the *Information Security Plan*.
Vulnerability Report	• Questionnaire detailing high-level vulnerability management practices such as how frequently entities perform penetration tests and patching.
Executive Acknowledgement of Risk	• Signed documentation that certain executive-level staff at reporting entities are informed of the risks identified in the self-assessment.
Data Security Plan for Online and Mobile Applications	• If an entity plans to create a website or mobile application processing certain confidential information, that entity must answer several questions detailing plans around application development, beta testing, penetration testing, and vulnerability testing.

To assist entities in gathering the data they need to complete their plans, DIR offers optional services like a penetration test, which is a deliberate attempt to circumvent security features to identify vulnerabilities, and the TCF Assessment, which is a third-party assessment of cybersecurity maturity against TCF standards, described in greater detail in the accompanying textbox.

Texas Cybersecurity Framework (TCF) Assessment

The Legislature has provided DIR funding to offer third-party cybersecurity assessments free of charge to eligible entities. Much like the self-assessment that entities perform for the *Information Security Plan*, these free assessments gauge an entity's cybersecurity against TCF standards. Obtaining a TCF Assessment gives entities an objective, outside view into their cybersecurity strengths and weaknesses and can help them fill out their *Information Security Plan*. DIR's current vendor, AT&T, performs assessments by:

- Collecting documentation of infrastructure and plans related to the TCF.
- Interviewing appropriate staff.
- Analyzing the data holistically to give a maturity score for each TCF security objective.
- Validating the entity's responses and putting together a list of recommendations and a roadmap showing different ways to implement recommendations based on cost and ease of implementation.

Once complete, the vendor sends the assessment report to the entity and DIR.

DIR sends three main biennial cybersecurity reports to the Legislature detailing entities' cybersecurity performance: the *Biennial Cybersecurity Report*, in which DIR assesses resources available to government entities to respond to cyberattacks, reviews existing statute, and makes recommendations; the *Consolidated Information Security Report*, a confidential report in which DIR analyzes the data that entities send through the *Information Security Plan* to identify trends, summarize statewide performance, and make

recommendations; and the *Consolidated Assessment of Agency IT Infrastructure*, another confidential report in which DIR scores agencies on their combined information technology (IT) and cybersecurity maturity.[5]

Statute also requires each entity to designate an information security officer (ISO) who has authority over the entity's information security.[6] ISOs complete biennial reporting requirements, notify DIR of security incidents, and act as the primary point of contact with DIR should a cyber incident requiring DIR's intervention arise.[7]

Findings

Low cybersecurity maturity among state entities increases risks to Texans.

If a state agency or institution of higher education does not have the processes and systems in place to protect its cybersecurity, the likelihood hostile actors will successfully target that entity increases, which could cost the state money, damage the state's reputation, and jeopardize Texans' privacy. Cyberattacks can be hugely expensive, and the amount of money organizations are forced to spend to respond to them has increased year after year. According to the Office of the Comptroller of Public Accounts, "more than 38,000 victims of cybercrime reported an estimated $313.6 million in financial losses in 2020 — an increase in losses of 42 percent from 2019 and 307 percent from 2016."[8] The 2020 SolarWinds cyberattack illustrates the scale of the challenge and danger. Sophisticated foreign attackers infiltrated a major network monitoring application's patching system, so when users updated to the latest version of that software, they inadvertently installed malware allowing the attackers access to their networks. Government agencies were among the victims of this attack, and the full scale of what the attackers were able to accomplish is still unknown.[9]

Cyberattacks can be hugely expensive.

Even cybersecurity failures at a few small agencies can pose significant risks to the state. One reason for this risk is that agencies may be responsible for holding personally identifiable information. For example, a regulatory agency with under 30 employees might store sensitive information about its license holders. Additionally, many government entities are interwoven with one another: if one agency is attacked, hackers could potentially access connected systems at another state agency. These and other problems stemming from seemingly isolated failures create a need for DIR to help ensure all state entities are meeting its cybersecurity standards.

DIR can present data demonstrating that the state performs better on cybersecurity than it used to and that Texas compares well to peer states, but some agency compliance records and TCF scores remain too low to adequately protect state systems.

Mandating independent, third-party assessments could improve the quality of information used for cybersecurity decision making.

The *Information Security Plans* entities send to DIR are one of DIR's most important sources of information regarding those entities' current levels of cybersecurity maturity. In addition to informing DIR's own approach to protecting the state, the facts DIR gathers from these *Information Security Plans* feed directly into the biennial reports the agency sends to the Legislature with recommendations for improving Texas' cybersecurity.[10] However, DIR does not verify the information it receives or require that entities use any objective third-party assessment, such as DIR's TCF Assessment, to inform their submissions.

DIR does not require entities to use an objective third-party assessment.

Obtaining independent, accurate, third-party assessments of agency cybersecurity is important because not all entities have the resources to hire staff who specialize in cybersecurity or IT, meaning not all ISOs may be able to answer *Information Security Plan* questions accurately and completely. While statute and rule require entities to appoint an ISO, many ISOs perform ISO duties as only a small component of their day-to-day work. Some entities appoint an ISO who works full-time as an executive director, administrative staff, or procurement specialist rather than appointing someone with a cybersecurity background or credentials.

ISOs with limited knowledge of cybersecurity still provide value as points of contact for DIR for reporting in cases of cybersecurity events, but these ISOs can struggle to understand the complex information they are required to report through the *Information Security Plan*. To illustrate this point, the textbox on the following page provides examples of DIR's description of the security objectives ISOs need to be able to understand and respond to for DIR to have the necessary information to make cybersecurity decisions and recommendations to the Legislature.[11]

- **Wider use of TCF Assessments could allow for verification of entity responses against a common standard.** DIR can gauge *Information Security Plan* accuracy when entities use information from the TCF Assessment, as both assess the same security objectives and score cybersecurity maturity according to the same rubric.[12] DIR's TCF Assessment uses an experienced, third-party vendor to assess an entity's cybersecurity, and DIR receives a copy of the final results of each TCF Assessment.[13] DIR could use these third-party cybersecurity maturity scores to confirm the accuracy of the scores the entity submits in its self-assessment for the *Information Security Plan*.

Information Security Plan - What ISOs Must Assess

The *Information Security Plan* asks ISOs to rank their entity's cybersecurity maturity on over 40 security objectives. Below are two objectives quoted from DIR's guidance documentation that may be a challenge for a non-specialist ISO to rate.

Security Objective: Secure Configuration Management

Definition: Ensures that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained throughout the respective system development life cycles. Establishes and enforces security configuration settings for information technology products employed in information systems. Ensures all systems are operating under configurations that have been agreed upon according to organizational risk management.

Security Objective: Security Monitoring and Event Analysis

Definition: Analysis of security events and alerts as detected by the array of security enforcement devices and log collection facilities implemented throughout the Enterprise environment. System level events include server operating system security and system logs. Application level events include web application logs, application access logs, and other application associated log events. Security monitoring and analysis includes alert configuration and generation, event correlation as well as defining and distributing periodic reports and event statistical analysis. Also includes analysis of events from the Internet content filtering system, SPAM prevention system, email encryption system, and other security control devices to ensure appropriate protections of information and information resources. Security Monitoring and Event Analysis can include advanced functionality used to detect fraud within program areas and ensure client identity protection by collecting and analyzing data access correlated with system events information. The limits of this function are limited only by the data sources that are compiled and the resources devoted to the data analysis.

- **Repeat TCF Assessments correlate with increased cybersecurity maturity.** DIR's data show that entities that obtain repeat TCF Assessments improve their overall cybersecurity maturity over time. Whether the assessments are directly responsible for the increases in maturity is unclear. However, a reasonable expectation is that at least some entities are using the knowledge and recommendations they gain from the assessments to drive improvements. Several entities that use the TCF Assessment expressed to Sunset staff that the assessment was useful.

Entities that obtain repeat TCF Assessments improve their cybersecurity maturity.

- **DIR could benefit from knowing when entities use non-DIR third-party assessments.** DIR does not have a formal mechanism for entities to report when they have used non-DIR third-party assessments similar to the TCF Assessment, such as assessments to evaluate compliance with federal cybersecurity standards for criminal justice data. Even if entities also use the TCF Assessment, having more data on the use of other assessments could help DIR better gauge the accuracy of entities' self-reported cybersecurity maturity and give it greater visibility into how entities protect their own cybersecurity.

DIR could better leverage legislative reporting to incentivize state agencies with the lowest cybersecurity maturity levels to improve.

- **Insufficient reporting to the Legislature.** As a non-regulatory agency, DIR cannot compel agencies to comply with its cybersecurity standards, but it can report to the Legislature on state agency compliance through the confidential *Consolidated Assessment of Agency IT Infrastructure*. This report acts as a scorecard for both IT and cybersecurity. DIR assigns agencies a combined score based on the following information submitted by the agency: the Information Resources Deployment Review (IRDR), *Information Security Plan*, the agency's most recent DIR-provided TCF Assessment and penetration test, security incident reporting, and IT inventory risks. DIR assigns 60 points total for the cybersecurity components and 40 points total for the IT components. In addition to providing summary information, DIR lists the worst-scoring agencies and reports on any remedial efforts those agencies inform DIR they are undertaking. The *Consolidated Assessment of Agency IT Infrastructure* does not include institutions of higher education because they do not submit full IRDRs.

  The Legislature may have incomplete information about agencies that have major cybersecurity shortcomings.

  While this scorecard helps inform the Legislature about struggling entities, it does not present a complete picture of every entity posing risks to the state through severe cybersecurity failures. The report presents a combined IT and cybersecurity score but does not provide separate IT and cybersecurity scores. IT and cybersecurity, while interconnected, are different fields with different risks and mitigation strategies. Combining IT and cybersecurity performance means the Legislature may have incomplete information about agencies that have major cybersecurity shortcomings but perform adequately on IT. For example, an agency could have low cybersecurity maturity yet no significant IT risks and would therefore rank higher in the consolidated report.

  In addition, DIR prioritizes TCF standards into high, medium, and low impact categories based on the potential impact of a failure of that security control. However, DIR does not proactively provide the Legislature information on which or how many entities rate zero or one out of five in its highest impact categories either in the consolidated report or any other report. Without such information, the Legislature cannot directly target struggling entities through enhanced oversight, legislation, or funding decisions for improvements.

- **No corrective action plans for agencies with the worst cybersecurity postures.** Statute requires agencies that fail to comply with DIR's rules, standards, state statute, or the *State Strategic Plan for Information Resources Management* to create corrective action plans detailing remedies, but DIR does not use this statutory mechanism to report that entities do not meet baseline cybersecurity standards.[14] Agencies convey a large amount of mainly IT information to DIR through the IRDR, described further in Issue 2, which DIR then reviews. While the IRDR includes some cybersecurity-

focused questions, the questions that require corrective action plans deal only with compliance with statute, such as whether an entity submitted its *Information Security Plan* and has appointed an ISO rather than how an agency performed on cybersecurity.[15] Illustrating the problem, an agency that scored itself zero out of five on every metric of cybersecurity maturity in the *Information Security Plan* would not need to submit a corrective action plan, so long as it achieved statutory compliance by submitting the plan. Not having corrective action plans for severe cybersecurity issues means agencies could go years without being required to create a plan to address problems, and the Legislative Budget Board and State Auditor's Office also would not be aware of these issues, as they receive status updates only on corrective action plans.

Some of DIR's statutory reporting requirements are duplicative and confusing, increasing the risk of entities not providing the right information needed to protect the state's cybersecurity.

- **Duplicative requirements.** Statute includes two separate reporting requirements that are largely duplicative.
  - The *Information Security Plan* requires entities to submit a self-assessment detailing their cybersecurity maturity and practices.[16]
  - The *Information Security Assessment* requires entities to submit a self-assessment of the information security of information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities.[17]

  In practice, these two reports provide DIR duplicative information, except that the *Information Security Assessment* includes an additional reporting requirement related to data governance, which continues to be needed. DIR collects information on this requirement separately from the *Information Security Plan* since data governance is a separate field from cybersecurity, and DIR receives important information from this component that it does not receive through any other provision of statute. DIR and reporting entities, including state agencies and institutions of higher education, would benefit from removing these duplicative reporting requirements and renaming the *Information Security Assessment* to reflect its data governance purpose.[18]

Existing, duplicative statutory language confuses reporting entities.

- **Confusing statutory language.** In addition to the *Information Security Assessment* required in statute, entities may voluntarily use DIR's third-party vendor to conduct an assessment of their cybersecurity maturity, known as the TCF Assessment. Using the same term "assessment" for the mandatory *Information Security Assessment* and the voluntary TCF Assessment is confusing and may create the impression that the TCF Assessment is the same as the requirement to perform a self-assessment of cybersecurity maturity. As part of the cybersecurity component of Sunset reviews, Sunset staff has encountered multiple entities that believed their

voluntary TCF Assessment was their mandatory *Information Security Plan* self-assessment, demonstrating that some entities are confused.

- **Conflicting deadlines.** Statute provides two deadlines for entities to submit the *Information Security Assessment* to DIR. Statute provides another deadline for the *Information Security Plan*, which acts as a third deadline for the same requirement since entities submit most of their *Information Security Assessment* materials through the *Information Security Plan* process.[19] The lack of a single deadline reduces clarity for reporting entities and increases their reporting burden while also making it more difficult for DIR to manage report intake.

- **Unnecessary security assessment of data governance.** One component of the *Information Security Assessment* requires entities to submit an information security assessment of its data governance program, but information security and data governance are distinct fields requiring different types of analysis. While an assessment of whether an agency's data governance program meets best practices could be useful, performing an information security assessment of data governance provides limited value to DIR.[20]

Sunset Staff Recommendations

Change in Statute

4.1 Require DIR to require state agencies under its jurisdiction to obtain a DIR-selected information security assessment periodically.

This recommendation would require DIR to require state agencies to undergo a third-party information security assessment of DIR's choosing — currently the TCF Assessment — periodically. DIR could perform these assessments itself or designate a vendor or vendors to perform the assessments on its behalf. DIR would be responsible for funding these assessments.

This recommendation would give DIR and, by extension, the Legislature more accurate information about state agencies' cybersecurity maturity. Requiring third-party assessments would also give agencies not currently using the TCF Assessment a better view into their own cybersecurity and how they could improve. This recommendation would not apply to institutions of higher education due to their relatively higher cybersecurity maturity status and, in the case of community colleges, due to how recently the Legislature placed them under DIR's jurisdiction. The recommendation would also not prevent state agencies from obtaining additional, non-DIR-provided third-party assessments.

4.2 Modify the existing *Information Security Assessment* reporting requirements to reduce redundancy.

This recommendation would remove all redundant components of the *Information Security Assessment* statute while retaining and clarifying the still useful requirement to perform assessments of data governance. Specifically, this would involve striking the redundant provision of statute that requires entities to submit a self-assessment of the information security of information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities since the *Information Security Plan* already requires entities to assess and report this information. This redundant

statute serves no valuable purpose and confuses reporting entities, so removing it would help ensure DIR and the Legislature receive complete and accurate information.

Additionally, this recommendation would clarify that the remaining requirement is a "data governance assessment" rather than an "information security assessment of data governance." By clarifying that the requirement would be for a data governance assessment according to best practices in that field, this recommendation adjusts statutory language to match current DIR practice. In alignment with Recommendation 4.3, the data governance assessment would be due June 1 of each even-numbered year.

4.3 Amend statute to change the deadline for submitting the *Information Security Assessment*.

This recommendation would remove conflicting due dates for the *Information Security Assessment* currently in statute and replace them with a requirement to submit reports to DIR by June 1 of each even-numbered year. This recommendation would strike the conflicting November 15 and December 1 deadlines currently in statute and replace them with a June 1 deadline to align with the deadline for the *Information Security Plan*. Moving the date to June 1 would give DIR sufficient time to review entities' submitted materials and form recommendations for the Legislature prior to the legislative session.

Changing statute in this manner would provide clarity to reporting entities, reduce the burden for them to meet competing deadlines in statute, and aid DIR in explaining reporting requirements to those entities.

Management Action

4.4 Direct DIR to create a mechanism for state agencies and institutions of higher education to report use of third-party assessments other than the TCF Assessment.

DIR should allow entities to report to DIR through the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management reporting tool when they have used a third-party cybersecurity assessment other than the TCF Assessment. This reporting mechanism could be a checkbox on the current *Information Security Plan* reporting tool or another mechanism but should include fields for these entities to name and describe the third-party cybersecurity assessment they used. DIR should also allow entities to securely and confidentially upload any copies of third-party assessments they wish to provide. Allowing entities to easily provide this information would improve DIR's awareness of state entities' cybersecurity posture overall.

4.5 Direct DIR to change certain processes related to entities reporting low cybersecurity maturity.

This recommendation would direct DIR to designate certain TCF security objectives as high priority. Currently, DIR lists four TCF standards as high impact but should include any other standards it deems necessary as high priority for the purposes of this recommendation. If an entity rated any of those objectives below a DIR-defined threshold in its *Information Security Plan*, DIR should send a letter to the agency or institution of higher education notifying the entity's leadership of the low maturity score and informing them of risks and any DIR assistance the entity is eligible to receive for free or at a cost.

This recommendation has additional components impacting only state agencies since institutions of higher education do not complete full IRDRs nor do they appear on the *Consolidated Assessment of Agency IT Infrastructure*. For state agencies, DIR should:

- Add a question to the IRDR asking if agencies scored any high priority objectives beneath a certain score on their last *Information Security Plan* that they have not mitigated. If an agency answers yes, DIR should require the agency to submit a corrective action plan.
- Provide the Legislature summary information on the number of entities meeting this criterion through one of DIR's existing confidential reports such as the *Consolidated Assessment of Agency IT Infrastructure* or *Consolidated Information Security Report*.

DIR should also adjust the *Consolidated Assessment of Agency IT Infrastructure* report to separate out scores for IT and cybersecurity. DIR could continue to provide the current consolidated scores in the report in addition to separate scores, if it chose to do so, but should clearly label them as such.

This recommendation would identify entities posing the greatest cybersecurity risks to the state; use existing mechanisms to ensure the Legislature, Legislative Budget Board, and State Auditor's Office are informed of those risks; and emphasize to noncompliant entities the seriousness of their cybersecurity risks.

Fiscal Implication

These recommendations could be implemented using current resources and would have no fiscal impact to the state. Recommendation 4.1 requiring state agencies to undergo a TCF Assessment periodically could be accomplished with existing resources because DIR has dedicated funding for that purpose. DIR provided TCF Assessments to several agencies in fiscal years 2022-23 and could use existing resources and funding to require the remaining agencies to obtain TCF Assessments periodically.

[1] DIR, *Self-Evaluation Report*, August 2023, p. 191, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[2] All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 2054.003, Texas Government Code; Section 2054.059, Texas Government Code.

[3] DIR, "Texas Cybersecurity Framework," accessed online March 15, 2024, https://dir.texas.gov/information-security/security-policy-and-planning/texas-cybersecurity-framework.

[4] National Institute of Standards and Technology, "About NIST," accessed online March 15, 2024, https://www.nist.gov/about-nist.

[5] Sections 2054.068(d), 2054.133(f), and 2054.0591, Texas Government Code.

[6] Section 2054.136, Texas Government Code.

[7] DIR, *Self-Evaluation Report*, August 2023, p. 236, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[8] Office of the Comptroller of Public Accounts, "Cybersecurity and Texas," *Fiscal Notes*, January 2022, accessed online March 27, 2024, https://comptroller.texas.gov/economy/fiscal-notes/archive/2022/jan/cybersecurity.php.

[9] DIR, *Self-Evaluation Report*, August 2023, p. 201, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf; Jennifer R. Franks, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, accessed online March 15, 2024, https://csrc.nist.gov/csrc/media/Presentations/2022/gao-report-federal-response-to-solarwinds/Franks%20-%20SolarWinds%20and%20MS%20Exchange%20Incidents%20-%203.9.2022%202pm.pdf.

[10] Section 2054.133(f), Texas Government Code.

[11] DIR, *Information Security Plan Template*, February 2022, accessed online February 19, 2024, https://dir.texas.gov/resource-library-item/information-security-plan-template.

[12] Ibid; DIR, *Self-Evaluation Report*, August 2023, p. 237, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[13] Ibid.

[14] Section 2054.097, Texas Government Code.

[15] DIR, *Information Resources Deployment Review 2024 Instructions*, accessed online March 15, 2024, https://dir.texas.gov/sites/default/files/2024-03/2024%20IRDR%20Instructions.pdf.

[16] Section 2054.133, Texas Government Code.

[17] Section 2054.515, Texas Government Code.

[18] DIR, *Self-Evaluation Report*, August 2023, p. 232, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[19] Sections 2054.515(b) and 2054.133(c), Texas Government Code; 1 Texas Administrative Code, Part 10, Chapter 218, Subchapter B, Section 218.10 (2023) (DIR, *Data Maturity Assessment*).

[20] DIR, *Self-Evaluation Report*, August 2023, p. 232, accessed online February 19, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

Issue 5

The State Has a Continuing Need for the Department of Information Resources.

Background

The Legislature established the Department of Information Resources (DIR) in 1989 to coordinate statewide information technology (IT) planning and monitor state agencies' acquisition of IT resources.[1] Since that time, the Legislature has significantly expanded DIR's powers and duties to include setting cybersecurity and data governance standards, overseeing the state's cybersecurity posture, providing telecommunications services directly and through contracts, and managing contracts for data center services and the state's website, Texas.gov. DIR also manages cooperative contracts through which state agencies, institutions of higher education, local governments, and other DIR customers purchase IT commodities, including software, hardware, and highly specialized staffing support. Eligible entities access DIR's services through a federated delivery model, in which DIR manages technology policy and shared, enterprise-level services while individual government entities manage their own day-to-day IT functions.

Findings

The state has a continuing need to coordinate IT procurement, IT planning, and cybersecurity to meet evolving constituent demands.

Texas needs modern, secure, and efficient government services to keep pace with the state's population growth, changing business environment, and constituent expectations. State agencies rely on IT systems for processing payments for government services; tracking and validating information for occupational licensing and other regulatory activities; managing complex projects; and determining eligibility for benefits and benefit delivery. DIR has helped modernize connections between government entities and the Texans they serve. For example, during the height of the COVID-19 pandemic, DIR responded to changing government needs by quickly providing IT infrastructure to make telework possible for state employees, enabling agencies and other entities to deliver crucial services in challenging circumstances. Within two weeks of the March 2020 disaster declaration, DIR strengthened the reliability of the state's internet and worked with 50 agencies that submitted roughly 4,000 service requests to increase work-from-home capacity.

DIR enables Texas government entities to harness the state's buying power to best serve their constituents.

- **Procurement.** DIR enables Texas government entities to harness the state's buying power, shared resources, and centralized IT procurement expertise to acquire and implement the goods and services they need to best serve their constituents. In fiscal year 2023, DIR managed approximately 800 cooperative contracts, through which vendors sold IT commodities to about 3,400 public entities, including local governments, schools, and institutions of higher education. According to DIR, these contracts generated $3.4 billion in sales and resulted in $399 million in cost savings for the customers of those public entities. DIR also renegotiated its Texas

DIR achieves cost savings by consolidating complex services.

Agency Network (TEX-AN) contracts in fiscal year 2022, increasing the number of telecommunications vendors available to its customers from five to 23. Through that expansion, DIR now provides state agencies, which are required to use TEX-AN contracts, and voluntary customers more purchasing options for telecommunications services, including a range of broadband services. DIR has also expanded the number of data center services offered through the Shared Technology Services (STS) program since fiscal year 2020 to include public and private cloud computing and storage services as well as technical solution design, delivery, and maintenance services. DIR currently manages 11 STS contracts that serve over 800 state and local entities with a total value of about $4 billion. Consolidating complex services enables DIR to achieve cost savings and negotiate standard terms and conditions that agencies may not be able to achieve on their own. For example, DIR estimates a small agency would need about $750,000 in startup costs and $2.4 million per year to maintain its own data center services infrastructure.[2] Through DIR's shared infrastructure, DIR estimates the same agency would need about $155,000 in startup costs and between $220,000 and $290,000 in annual maintenance for data center services.[3]

- **IT planning.** By coordinating statewide IT planning, DIR helps ensure Texas state agencies and institutions of higher education have coordinated goals to keep pace with advances in technology and deliver a better government experience for Texans.[4] The accompanying textbox summarizes the state's current IT goals and guiding principles DIR identified through its *State Strategic Plan for Information Resources Management*.[5] In addition to publishing the state strategic plan, DIR ensures the Legislature has the information it needs to make future IT funding and policy decisions by reporting on state agency progress toward IT and cybersecurity goals, making recommendations to the Legislature for improving the cost effectiveness and efficiency of the state's use of information resources through the *Biennial Performance Report*, and identifying the IT projects that most need funding through the *Prioritized Cybersecurity and Legacy Systems Report*.[6] The state benefits from this coordinated planning and reporting function as it ensures the Legislature has a global view of the state's progress on IT, promotes the adoption of common IT best practices, and helps ensure Texas governmental entities acquire and maintain secure, efficient, and modern IT systems.

***State Strategic Plan* Guiding Principles and Goals, FYs 2024-28**

Guiding Principles: Prioritize security, focus on Texans, and collaborate.

Goal 1
Elevated government experience

Goal 2
Mature data management and privacy practices

Goal 3
Skilled and resilient workforce

Goal 4
Transformation and modernization

- **Cybersecurity.** DIR's coordination of statewide cybersecurity through security operations centers across the state, endpoint detection and response, and other cybersecurity services ensures the state can keep pace with evolving threats that are expensive to mitigate. Cybersecurity threats are increasingly common, sophisticated, and costly, and they impact all levels

of government — federal, state, and local. In 2023, a public sector data breach cost an average of $2.6 million to mitigate.[7] DIR also serves a vital role coordinating statewide cybersecurity incident response and collaborates with state agencies and federal partners such as the U.S. Department of Homeland Security and the FBI to protect the state's critical infrastructure from cybersecurity attacks. Since 2020, DIR has assisted public entities in responding to more than 90 ransomware attacks.

Cybersecurity threats are increasingly common, sophisticated, and costly.

No substantial benefits would result from transferring DIR's functions to a different state agency.

Sunset staff considered organizational alternatives for administering DIR's programs but concluded no significant benefit would result from transferring functions or merging DIR with the state's other procurement or cybersecurity-related agencies: the Statewide Procurement Division (SPD) at the Office of the Comptroller of Public Accounts, the Office of the Attorney General (OAG), and the Texas Department of Public Safety (DPS).

While SPD also procures commodities on behalf of state agencies and other public entities, IT procurement requires specialized expertise in highly technical, complex, and rapidly changing fields. Transferring DIR's IT commodities procurement function to SPD would result in a one-to-one transfer of resources and gain no administrative efficiencies because, in addition to IT commodities, DIR also procures products and services for the agency's STS program, and both programs rely on other DIR divisions for subject matter expertise. For example, DIR's in-house cybersecurity subject matter experts help ensure the agency procures effective and secure solutions to improve the state's security posture. DIR and SPD maintain an effective division of responsibilities, with DIR focusing on IT commodities such as computers or software and SPD focusing on non-IT goods and services such as vehicles or furniture. SPD and DIR meet regularly to avoid overlap in commodities procurement.

In addition, DIR centralizes support for Texas government entities to address cybersecurity incidents and acquire commodities and services necessary to improve their cybersecurity posture. Within an agency, IT and cybersecurity functions can conflict because IT prioritizes system performance and usability, while cybersecurity focuses on protecting those systems, which can affect functionality and user experience. However, from a statewide perspective, having these functions housed in a single agency benefits the state. DIR's coordination of IT and cybersecurity provides the state a more holistic picture of the systems currently used by government entities and the risks they pose, which can help the Legislature target funding and other improvements. At the same time, DIR's planning for future IT needs highlights emerging technologies and the potential benefits and threats those technologies will bring. The structure also provides a unified approach when incidents occur, as DIR can both respond to the incident and also help steer agencies and other entities to products and services that could prevent future incidents. Although both OAG and DPS

DIR's coordination of IT and cybersecurity provides the state a more holistic picture of risks.

Cybersecurity Functions - DPS and OAG

DPS

- Investigates cybercrimes.
- Assists law enforcement agencies with cybersecurity incident response.

OAG

- Prosecutes cybercrimes.
- Enforces laws addressing data breaches through lawsuits.
- Provides processes to submit consumer complaints and catastrophe notices related to data breaches and cybersecurity incidents.

IT Service Delivery Model Definitions

- **Federated:** A single entity coordinates certain IT functions for public entities as shared services, with other functions managed individually by each entity.
- **Centralized:** A single entity provides IT services to each agency.
- **Decentralized:** Each agency independently manages its own IT services.

have responsibilities related to cybersecurity, as detailed in the accompanying textbox, their missions encompass much more than that, and taking on DIR's responsibilities would unnecessarily distract from their other primary responsibilities.[8]

While organizational structures and service delivery models vary, all 50 states have information technology and cybersecurity functions.

All states coordinate oversight of technology operations and strategy in a statewide leadership position through a chief information officer (CIO) or similar position. In Texas and 23 other states, a CIO or equivalent operates in an independent agency, while 20 state CIOs serve in a division of a larger agency and six state CIOs reside in the governor's office. CIOs typically use one of three approaches to delivering IT services to state agencies, which are defined in the *IT Service Delivery Model Definitions* textbox.[9] Texas and 26 other states follow the federated model, 16 states follow the centralized model, and seven states follow the decentralized model, as shown in the *Service Delivery Models of IT Functions in Other States* textbox.[10] Similar to Texas, 32 other states house their cybersecurity prevention and response under the state's CIO, while the organizational structures of the remaining states vary.

Service Delivery Models of IT Functions in Other States - 2023

Federated: 27
Arkansas, California*, Colorado*, Connecticut*, Delaware, Georgia, Hawaii, Idaho*, Illinois, Indiana, Iowa, Kansas, Kentucky, Maryland, Massachusetts, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania*, South Carolina, Tennessee*, Texas, Virginia*, Wisconsin

Centralized: 16
Louisiana, Maine, Michigan, Minnesota, Missouri, Nebraska, New Hampshire, New York, North Dakota, Oklahoma, Rhode Island, South Dakota, Utah, Vermont, West Virginia, Wyoming

Decentralized: 7
Alabama, Alaska, Arizona, Florida, Mississippi, New Mexico, Washington

* In 2022, the Center for Digital Government (CDG) surveyed state governments on how state agencies receive IT services using one of three delivery models: centralized, decentralized, and federated. Asterisks indicate the state's 2023 delivery model changed since 2022, based on CDG's and Sunset staff's updated research.

DIR has three reporting requirements that need to be eliminated or modified.

The Sunset Act establishes a process for the Sunset Commission to consider if reporting requirements of agencies under review need to be continued or abolished.[11] The Sunset Commission has interpreted these provisions as applying to reports that are specific to the agency and not general reporting requirements that extend well beyond the scope of the agency under review. Reporting requirements with deadlines or that have expiration dates are not included nor are routine notifications, notices, or posting requirements.

Statute requires DIR to produce 16 reports specific to the agency, as listed in Appendix G. Of these 16, Sunset staff found that two reports contain outdated reporting requirements and need to be modified and one should be eliminated.

- ***Biennial Performance Report.*** In 2007, the Legislature added a requirement to DIR's *Biennial Performance Report* for the agency to provide a summary of internet-based training provided by state agencies and institutions of higher education.[12] However, since that time, most state agencies and institutions of higher education have begun providing online options for most trainings. Statute should be updated to reflect that this aspect of the reporting requirement is no longer needed.

- ***State Strategic Plan for Information Resources Management.*** Statute requires DIR to incorporate in the *State Strategic Plan for Information Resources Management* efficiencies obtained through shared transmission services and open systems architecture as they become available.[13] Since the Legislature added this language to DIR's governing statute in 1997, these services have become standard in telecommunications, making this aspect of the reporting requirement outdated and no longer needed.

- **Report on the Placement of Information Resource Managers (IRMs) in Agency Hierarchies.** Statute requires DIR to continually inform the Legislature of the placement of IRMs in agency hierarchies.[14] DIR does not produce this report in practice because the agency already receives IRM placement information through the Information Resource Deployment Review, the results of which DIR reports to the Legislature through the *Biennial Performance Report*, so this report is no longer needed.

The agency's statute does not use appropriate language when referring to persons with disabilities.

Statute requires Sunset to consider and recommend, as appropriate, statutory revisions in accordance with the person-first respectful language outlined in general law.[15] The stated intent of the law is to try to affect society's attitudes toward people with disabilities by changing the way the language refers to them. Sunset only changes language that occurs in chapters of law that are opened by the Sunset Commission's recommendations.

The governing statute for DIR contains terms that are not consistent with the person-first respectful language initiative. The agency's Sunset bill should revise the statute to use person-first respectful language when appropriate.

DIR does not adequately document its risk assessment process and could benefit from additional board member input to ensure DIR appropriately identifies the highest risks to the agency.

Explicitly including STS in its risk assessment would ensure DIR accounts for major risks.

Statute requires DIR's board to appoint an internal auditor to report directly to the board and requires the auditor to prepare an annual audit plan subject to board approval, using risk assessment techniques to rank the agency's high-risk functions.[16] While DIR has a broad risk assessment methodology reviewed by agency leadership and the board, as defined in the accompanying textbox, DIR could not provide documentation of how it used risk assessment criteria to arrive at its ranking of risks to the agency, such as scoring of interview responses or an evaluation of a program's importance in meeting the agency's strategic goals. DIR's two most recent risk assessments — for fiscal years 2023 and 2024 — also lacked an evaluation of the risk of DIR's STS contracts, other than Texas.gov and public cloud, though STS represents a contract value of over $4 billion and the program's failure would significantly affect DIR's ability to carry out its mission. While the State Auditor's Office recently audited certain STS contracts and DIR regularly audits STS contracts for compliance with federal requirements, explicitly including STS in its risk assessment documentation would ensure DIR accounts for the major risks associated with this key function.

DIR Internal Audit Plan, Risk Assessment Methodology - FY 2024

The audit plan risk assessment process incorporates input from key staff members, including the executive leadership team, who were interviewed to determine risks in their areas and to the agency. The process also involved reviewing various documents, including:

- Organizational charts
- Policies and procedures
- Prior internal and external audit reports and risk assessments
- DIR's *Strategic Plan*
- Applicable laws and rules

The risk assessment:

- Identifies high risk areas that are not included in the audit plan due to variables outside of agency control.
- Provides that risks within the agency's control but not included on the audit plan should be addressed by the agency through adequate internal controls.

In addition, unlike several other agencies such as the Teacher Retirement System of Texas, Public Utility Commission of Texas, and Texas Department of Public Safety, DIR's internal auditor does not individually interview board members to inform the audit plan, though board members review and approve the plan's final version. Because DIR's internal audit function is mostly outsourced and has had problems identified in previous Sunset reports, DIR could benefit from using the board's insight on which programs to audit before the audit plan is written.

Sunset Staff Recommendations

Change in Statute

5.1 Continue the Department of Information Resources for 12 years and remove the Sunset date of the agency's enabling statute.

This recommendation would continue the Department of Information Resources until September 1, 2037, and would also remove the Sunset date of the agency's statute to ensure only the agency, not its statute, expires.

5.2 Abolish one, modify two, and continue 13 of DIR's reporting requirements.

This recommendation would eliminate the requirement for DIR to publish a report on the placement of IRMs in agency hierarchies. DIR would still receive this information in the Information Resources Deployment Review and could publish it in the *Biennial Performance Report*. This recommendation would also remove the requirement that DIR provide a summary of the amount of internet-based training provided by each state agency and institution of higher education in the *Biennial Performance Report* as well as the requirement to include information in the *State Strategic Plan for Information Resources Management* on efficiencies associated with the use of shared transmission systems and open systems architecture. Both of these requirements are outdated and no longer necessary.

5.3 Update DIR's statute to reflect the requirements of the person-first respectful language initiative.

This recommendation would direct the Texas Legislative Council to revise DIR's statute to conform to the person-first respectful language requirements found in Chapter 392, Texas Government Code.

Management Action

5.4 Direct DIR to document its ranking of risks identified in the audit plan and interview the board to inform the audit plan.

Under this recommendation, DIR's internal auditor should document how they ranked the risks of each program area in risk assessment, including how DIR evaluated and scored responses to interviews and the importance of certain program areas in meeting strategic goals identified in the *State Strategic Plan for Information Resources Management*. The internal auditor should also seek input from board members regarding areas to audit before developing the fiscal year 2025 audit plan and in future plans. Documenting its risk assessment methodology and incorporating board member input will help ensure DIR and its board have better visibility, control, and oversight of the agency's risks and any risks to the state's IT operations.

Fiscal Implication

Continuing the Department of Information Resources would require an annual appropriation from the Legislature, which was approximately $680 million per year for the 2024-25 biennium. These recommendations could be accomplished with existing resources and would not result in a fiscal impact to the state.

[1] Chapter 788 (HB 2736), Acts of the 71st Texas Legislature, Regular Session, 1989.

[2] DIR, *Self-Evaluation Report*, August 2023, p. 299, accessed online April 29, 2024, https://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

[3] Ibid.

[4] DIR, *2024-2028 State Strategic Plan for Information Resources Management*, p. 1, accessed online March 21, 2024, https://dir.texas.gov/sites/default/files/2023-10/2024-2028%20State%20Strategic%20Plan%20for%20Information%20Resources%20Management.pdf.

[5] DIR, *Quick Reference Guide: Next-Level Tech for an Exceptional Government Experience*, accessed online March 21, 2024, https://dir.texas.gov/sites/default/files/2023-11/2024-2028%20State%20Strategic%20Plan%20for%20Information%20Resources%20Managment%20Quick%20Reference%20Guide.pdf.

[6] DIR, *2022 Biennial Performance Report: Accelerating the Next Generation of Technology in Texas*, p. 2, accessed online March 21, 2024, https://dir.texas.gov/sites/default/files/2022-11/2022%20Biennial%20Performance%20Report.pdf; DIR, *Prioritized Cybersecurity and Legacy Systems (PCLS) Study Report to the Legislative Budget Board*, p. 3, accessed online March 21, 2024, https://dir.texas.gov/sites/default/files/2022-10/2022%20PCLS%20Public%20Report.pdf.

[7] IBM, *Cost of a Data Breach Report 2023*, p. 13, Figure 4, accessed online February 28, 2024, https://www.ibm.com/downloads/cas/E3G5JMBP.

[8] Office of the Attorney General, *Agency Strategic Plan Fiscal Years 2023-2027*, June 1, 2022; Texas Department of Public Safety, *Agency Strategic Plan Fiscal Years 2023 to 2027*, June 6, 2022.

[9] Jessica Mulholland, "Navigating the Road to Consolidation," Government Technology, August 10, 2015, accessed online March 3, 2024, https://www.govtech.com/computing/navigating-the-road-to-consolidation.html.

[10] Janet Grenslitt, "Digital States Survey 2022 Results Announced," Center for Digital Government, September 29, 2022, accessed online March 1, 2024, https://www.govtech.com/cdg/digital-states/digital-states-survey-2022-results-announced.

[11] All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Sections 325.0075, 325.011(13), and 325.012(a)(4), Texas Government Code.

[12] Section 2054.055(b)(8), Texas Government Code.

[13] Section 2054.0925(c), Texas Government Code.

[14] Section 2054.075(b), Texas Government Code.

[15] Section 325.0123, Texas Government Code.

[16] Section 2054.038, Texas Government Code.

Appendix A | Customer Use of DIR Services

During the 88th Legislative Session, the Legislature amended customer eligibility for the Department of Information Resources' (DIR) services, allowing all entities in the table below to use DIR services if DIR's executive director determines that it is in the best interest of the state.[1] While eligible, not all customer types use every DIR service. The following table illustrates which customer types are currently using various DIR services. State agencies are required to use the services shaded in beige unless they receive an exemption from DIR.

	Cooperative Contracts	Bulk Purchasing	Communications Technology Services			Shared Technology Services				
			TEX-AN (DIR-billed)	TEX-AN (Vendor-billed)	CCTS	Data Center Services	Managed Security Services	Texas.gov	Open Data Portal	Print, Mail, and Digitization
State Agencies	✓	✓	✓	✓	✓	✓[2]	✓	✓	✓	✓
Private Institutions of Higher Education	✓		✓	✓						
Public Institutions of Higher Education	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Public K-12 Schools	✓		✓	✓			✓			
Private K-12 Schools	✓									
Open Enrollment Charter Schools	✓		✓	✓			✓			
The Legislature and Legislative Agencies	✓		✓	✓	✓					
Courts	✓		✓	✓	✓					
Local Governments	✓	✓	✓	✓		✓	✓	✓	✓	✓

Appendix A

	Cooperative Contracts	Bulk Purchasing	Communications Technology Services			Shared Technology Services				
			TEX-AN (DIR-billed)	TEX-AN (Vendor-billed)	CCTS	Data Center Services	Managed Security Services	Texas.gov	Open Data Portal	Print, Mail, and Digitization
River Authorities	✓	✓	✓	✓		✓	✓	✓		
Public Safety Entities										
Volunteer Fire Departments	✓			✓						
Public Hospitals	✓	✓	✓	✓		✓	✓			
Electric Reliability Council of Texas	✓									
Texas Permanent School Fund Corporation	✓		✓	✓	✓	✓	✓			
Assistance Organizations	✓		✓	✓			✓			
Other States' Governmental Entities	✓			✓						

1 All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Chapter 242 (HB 4553), Acts of the 88th Texas Legislature, Regular Session, 2023.

2 Data Center Services has 25 designated customers that are required to participate; other state agencies are voluntary customers.

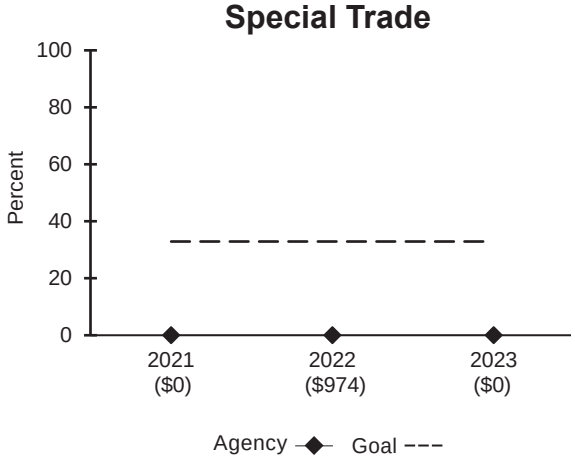
Appendix B

Historically Underutilized Businesses Statistics, FYs 2021-23

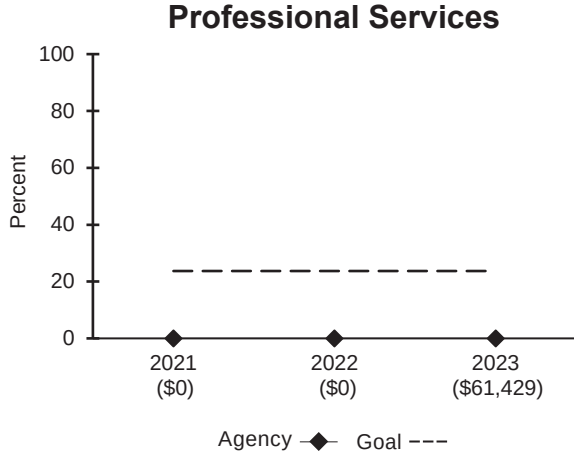
The Legislature has encouraged state agencies to increase their use of historically underutilized businesses (HUBs) to promote full and equal opportunities for all businesses in state procurement. The Legislature also requires the Sunset Commission to consider agencies' compliance with laws and rules regarding HUB use in its reviews.[1]

The following material shows trend information for the Department of Information Resources' (DIR) use of HUBs in purchasing goods and services. The agency maintains and reports this information under guidelines in statute.[2] In the charts, the dashed lines represent the goal for HUB purchasing in each category, as established by the comptroller's office. The diamond lines represent the percentage of agency spending with HUBs in each purchasing category from fiscal years 2021-23. Finally, the number in parentheses under each year shows the total amount the agency spent in each purchasing category.

The agency exceeded statewide purchasing goals for the other services category in all three fiscal years from 2021-23. The agency had no spending in the heavy construction and building construction categories in all three fiscal years from 2021-23. The agency had varied results for the commodities category for the same time period. The agency has not met the statewide goals in the professional services category in fiscal year 2023 and in the special trade category in fiscal year 2022.

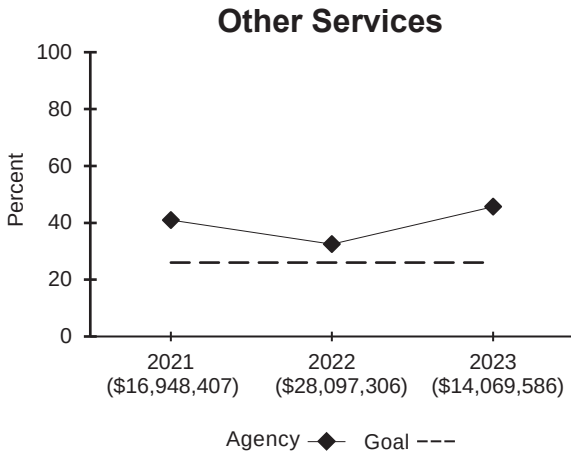


The agency had little to no special trade spending in each of the last three fiscal years. In fiscal year 2022, the agency fell short of the statewide goal for spending in special trade but spent a total of only $974 on an emergency purchase of security system parts.

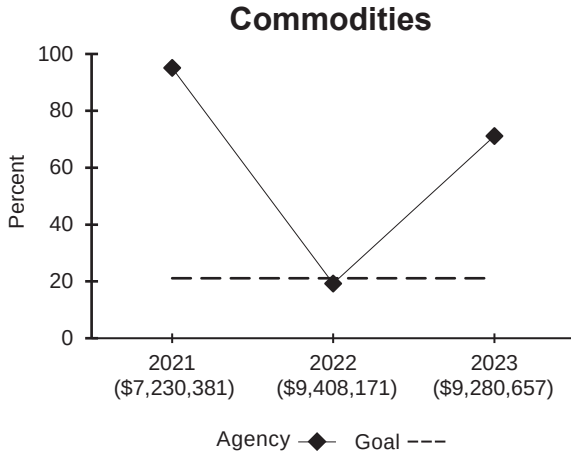


The agency had no professional services spending in fiscal years 2021 and 2022. The agency fell short of the statewide goal for spending in professional services in fiscal year 2023. However, the agency had limited opportunities for HUB spending in this category because no HUB vendors responded to the agency's professional services solicitations in fiscal year 2023.

Appendix B



The agency exceeded the statewide goal for spending in other services in each of the last three fiscal years.



The agency exceeded the statewide goal for spending in commodities in fiscal years 2021 and 2023 but fell short in fiscal year 2022.

[1] All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 325.011(9)(B), Texas Government Code.

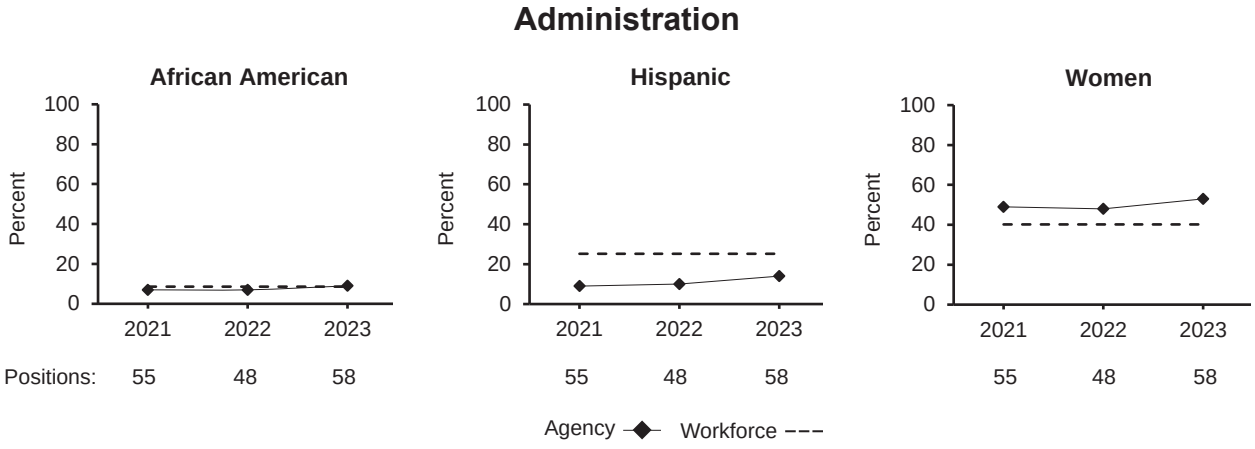
[2] Chapter 2161, Texas Government Code.

Appendix C

Equal Employment Opportunity Statistics, FYs 2021-23

In accordance with the requirements of the Sunset Act, the following material shows trend information for the employment of minorities and women in all applicable categories by the Department of Information Resources.[1] The agency maintains and reports this information under guidelines established by the Texas Workforce Commission.[2] In the charts, the dashed lines represent the percentages of the statewide civilian workforce for African Americans, Hispanics, and women in each job category.[3] These percentages provide a yardstick for measuring agencies' performance in employing persons in each of these groups. The diamond lines represent the agency's actual employment percentages in each job category from fiscal years 2021-23.

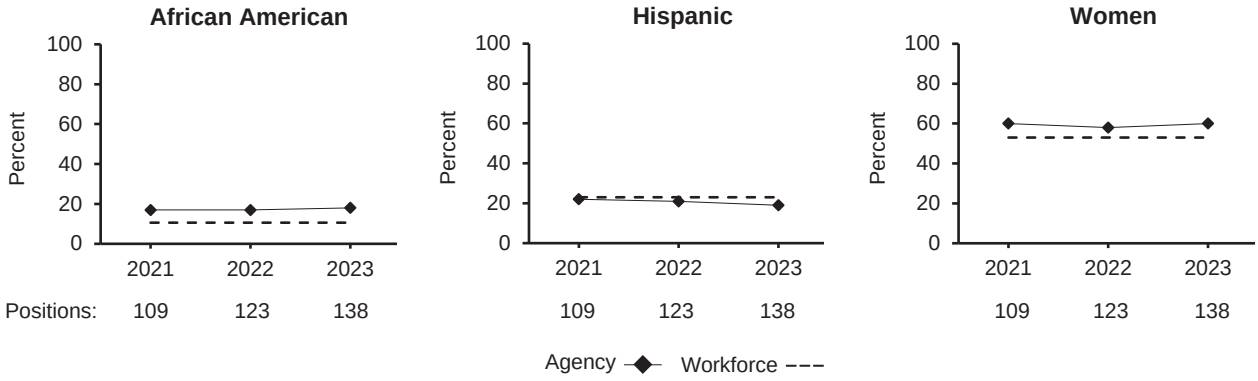
The agency exceeded statewide civilian workforce percentages for African Americans and women in several categories over the last three fiscal years. The agency failed to meet statewide civilian workforce percentages for Hispanics in almost all categories over the last three fiscal years. The agency had no employees in the skilled craft and protective services categories and too few employees in the service/maintenance category to conduct a meaningful comparison to the overall civilian workforce.



The agency exceeded statewide civilian workforce percentages for women in each of the last three fiscal years but fell short for percentages of Hispanics in each of the last three fiscal years. The agency failed to meet statewide civilian workforce percentages for African Americans in fiscal years 2021 and 2022 but exceeded percentages in fiscal year 2023.

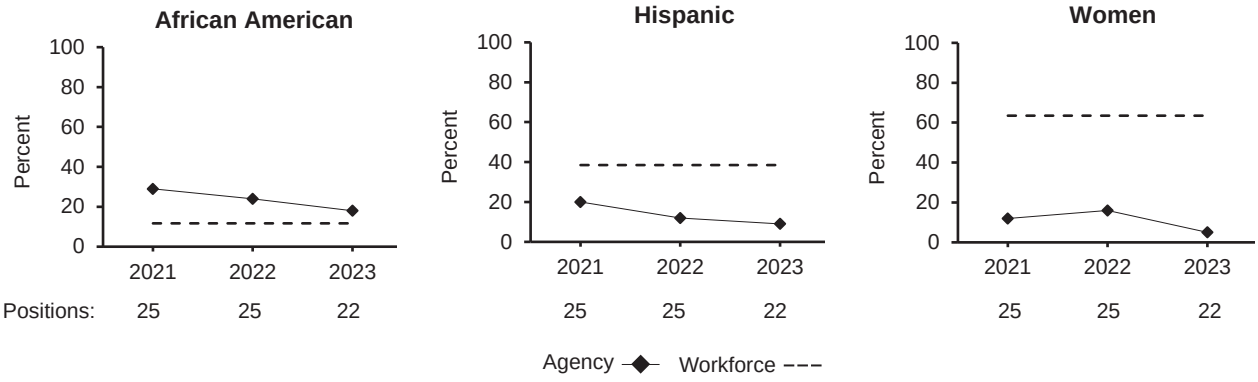
Appendix C

Professional



The agency exceeded statewide civilian workforce percentages for African Americans and women in each of the last three fiscal years. The agency exceeded statewide civilian workforce percentages for Hispanics in fiscal year 2021 but fell short in fiscal years 2022 and 2023.

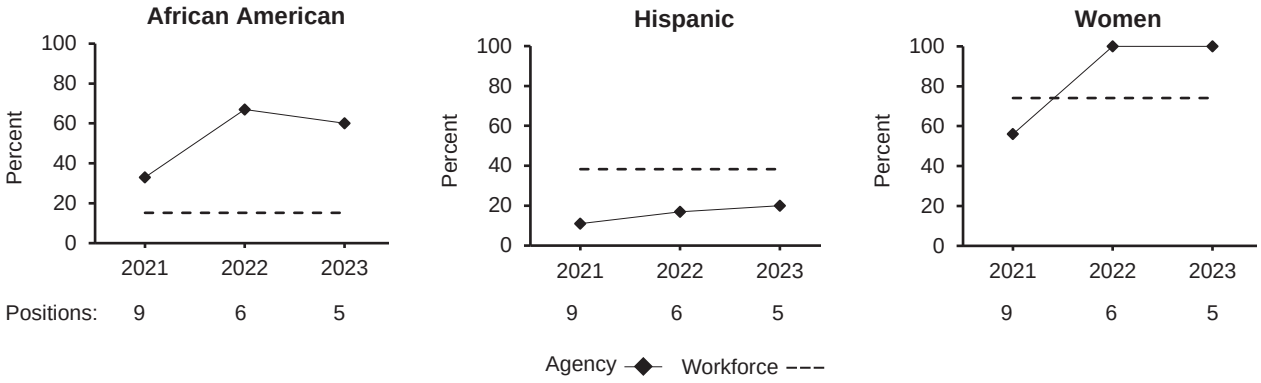
Technical



The agency exceeded statewide civilian workforce percentages for African Americans in each of the last three fiscal years but fell short for percentages of Hispanics and women in each of the last three fiscal years.

Appendix C

Administrative Support



The agency exceeded statewide civilian workforce percentages for African Americans in each of the last three fiscal years, but fell short for percentages of Hispanics in each of the last three fiscal years. The agency exceeded statewide civilian workforce percentages for women in fiscal years 2022 and 2023 but fell short in fiscal year 2021.

1 All citations to Texas statutes are as they appear on http://www.statutes.legis.texas.gov/. Section 325.011(9)(A), Texas Government Code.

2 Section 21.501, Texas Labor Code.

3 Based on the most recent statewide civilian workforce percentages published by the Texas Workforce Commission.

Appendix D

Shared Technology Services (STS) Delivery Model

The Multi-sourcing Services Integrator (MSI) gives customers a single point of entry into all STS programs. The Department of Information Resources contracts with an MSI vendor to manage and integrate STS for customers, standardize processes, administer enterprise service components, and maintain the STS Customer Portal.[1]

MSI
Capgemini

- Marketplace
- Business Management
- Customer Relationship Management
- Service Management
- Operations Management

Data Center Services

- Texas Private Cloud - Atos
- Public Cloud Manager - Rackspace
- Mainframe Services - Atos
- Technology Solution Services - Deloitte
- Application Services - Deloitte
- Print, Mail, Digitization - Xerox
- Security Operations - SAIC

Texas.gov
Deloitte and Tyler Technologies

- Constituent Payment Portal Applications
- Statewide Internet Portal
- Texas by Texas (TxT)

Managed Security Services
AT&T

- Device Monitoring
- Incident Response
- Assessments

Open Data Portal
Tyler Technologies

- Official State Repository of Publicly Available Electronic Data

[1] Department of Information Resources, *Self-Evaluation Report*, August 2023, p. 292, accessed online March 14, 2024, hhttps://www.sunset.texas.gov/public/uploads/2023-10/~Texas%20Department%20of%20Information%20Resources%20Self-Evaluation%20Report%202024-2025_Corrected.pdf.

Appendix E

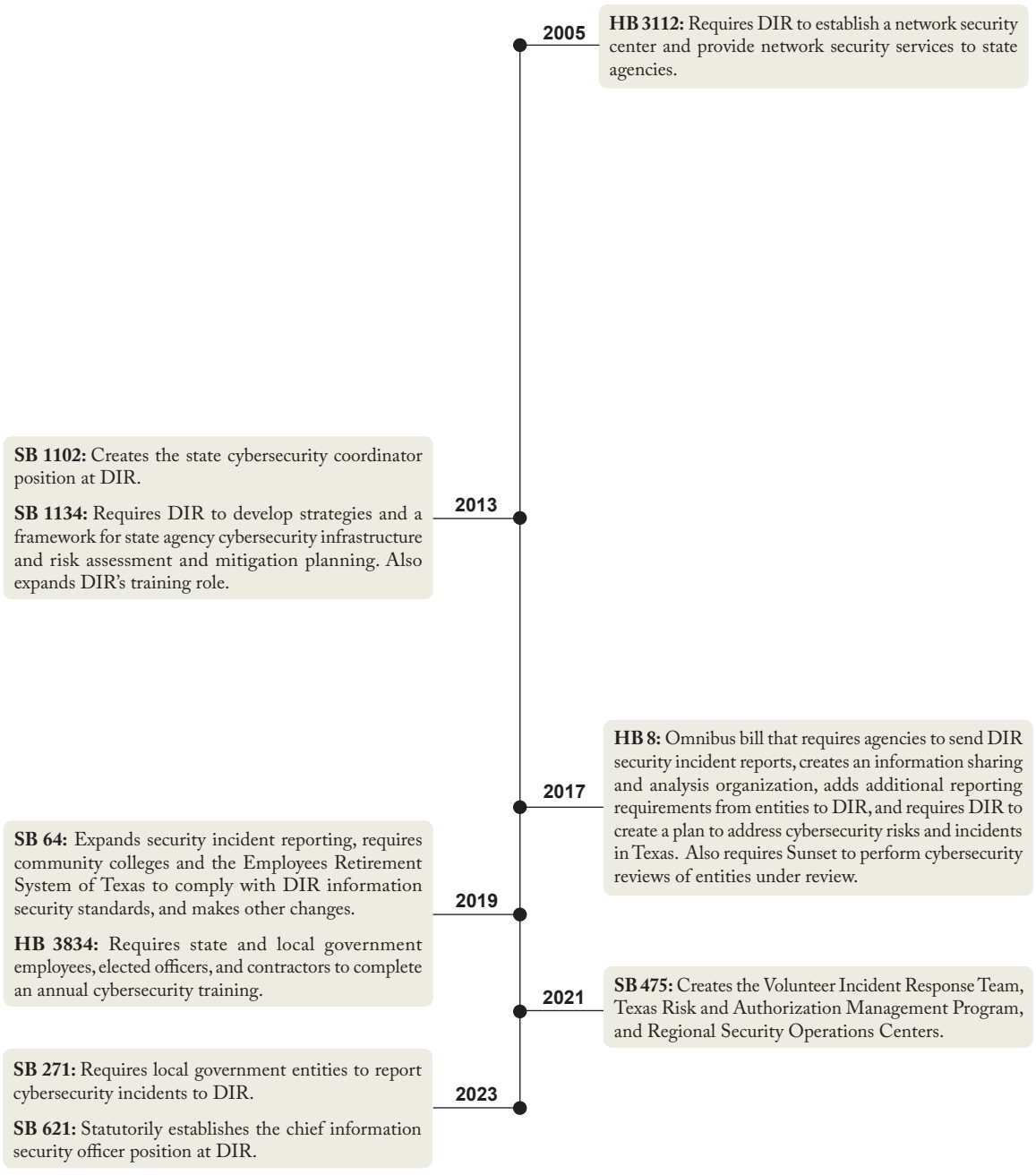
Shared Technology Services (STS) Governance Groups

Group	Membership	Purpose
STS Data Center Services (DCS) Partner Groups	Five customer partner groups composed of STS customers, primarily state agencies.	Customer partner groups meet periodically to identify and discuss issues or ideas to bring to governance committees and solution groups for consideration.
Business Executive Leadership Committee (BELC)	One representative (executive director, deputy executive director-level, or designee) from each Department of Information Resources (DIR) STS customer partner group described above, one representative from each of the three agencies with the largest DCS appropriation projected for the current biennium, one representative from each of the two agencies with the largest Texas.gov projected transaction revenues for the current biennium, two at-large members (one to represent small-sized customers consuming DCS infrastructure management and one to represent STS optional services customers), the DIR executive director, DIR chief of staff or equivalent position, and DIR chief operating officer.	Establishes enterprise business strategy and objectives for the STS program and monitors achievement. The committee also resolves strategic program business issues escalated by the Information Technology (IT) Leadership Committee.
IT Leadership Committee (ITLC)	One representative from each customer partner group, one representative from DIR, one representative from the Multi-sourcing Services Integrator (MSI), one representative from each related Service Component Provider (SCP), and one designated representative from the Texas Health and Human Services Commission. ITLC members are IT directors, information resources managers, chief information officers, or commensurate.	Defines enterprise technology strategic goals for STS and promotes their achievement. The committee has approval rights over critical IT decisions, resolves issues escalated by solution groups, and addresses appeals to solution group decisions.
Private Cloud and Mainframe Solution Group	One representative from each customer partner group, one representative from DIR, one representative from the MSI, and one representative from each related SCP.	Establishes policies, sets priorities for development of new services, establishes standards, and resolves issues related to private cloud services.
Public Cloud Solution Group	One representative from each customer partner group, one representative from DIR, one representative from the MSI, and one representative from each related SCP.	Establishes policies, sets priorities for development of new services, establishes standards, and resolves issues related to public cloud services.

Appendix E

Group	Membership	Purpose
Technology Solution Services (TSS) Solution Group	One representative from each customer partner group, one representative from DIR, one representative from the MSI, and one representative from each related SCP.	Reviews and provides feedback on DCS policies, evaluates and provides direction on DCS operations, resolves technical and operational issues related to DCS delivery, recommends changes to DCS, and provides guidance to service providers concerning customer needs and priorities for development of new services, setting priorities for service evolution, establishing standards, and resolving issues.
Geographic Information Systems (GIS) Solution Group	Nine members from agencies that directly contribute to the purchase of Statewide High Resolution Imagery Services, GIS data, GIS software, or any other GIS solution procured through STS.	Defines enterprise GIS technology strategic goals for implementation through STS and the Geographic Information Office to promote goal achievement. The committee has approval rights over critical GIS technology decisions.
Contracts and Finance Solution Group	Seven members, including one representative from each partner group and two representatives from DIR (one from Contracts and one from Finance).	Promotes effective enterprise contract and financial management in the DCS program by reviewing and soliciting DCS customer perspective on contractual or financial management issues.
Security Solution Group	One information security officer representative from each partner group, two IT directors designated at-large by the ITLC, one representative from DIR, one representative from the MSI, and one representative from each related SCP.	Oversees enterprise security related activities, monitors security performance trends, and addresses enterprise security issues and gaps related to STS in the context of DIR's rules regarding information security standards.
Texas Digital Identity Solution (TDIS) User Group	Agencies that directly contribute to TDIS by opting into the multi-factor authentication (MFA) platform and make configuration decisions for their agency.	Serves as a forum to present and discuss the development and delivery of MFA services within STS.
Print, Mail, and Digitization User Group	Twelve state agency members including one DIR staff member.	Serves as a forum to present and discuss the development and delivery of bulk print, mail, and digitization services and service options within STS.
Texas.gov Solution Group	One DIR representative, one representative from the Office of the Comptroller of Public Accounts, and one representative from each agency that directly contributed to the identification and development of Texas.gov-hosted applications and solutions procured through STS.	Coordinates stakeholder interests in transforming digital business using the Texas.gov website or web and mobile application Texas by Texas (TxT), establishes criteria to prioritize program investments using Texas.gov transaction revenue, and addresses enterprise Texas.gov service delivery issues and gaps.

Appendix F | DIR Cybersecurity Legislative History



Appendix G | DIR Reporting Requirements

Report Title	Legal Authority	Description	Recipient	Sunset Evaluation
1. Report on Administrative Fees	Section 2054.0346, Texas Government Code	Requires DIR to annually report all administrative fees that DIR sets each fiscal year, including the methodology and analysis used to determine the fee amounts and the cost allocation charged to customers.	Legislative Budget Board	Continue
2. Biennial Performance Report on the Use of Information Resources Technologies by Texas State Agencies	Sections 2054.055 and 2054.157(b), Texas Government Code	Requires DIR to biennially report on the use of information resources technologies by state government. Among other aspects, DIR must assess the state's progress toward meeting goals identified in the latest *State Strategic Plan for Information Resources Management*, describe major problems in information resources management confronting the state, and provide a summary of the amount and use of internet-based training provided by state agencies and institutions of higher education.	Governor and Legislature	Modify - See Recommendation 5.2
3. Biennial Cybersecurity Report	Section 2054.0591, Texas Government Code	Requires DIR to biennially report on resources available to government entities to respond to cyberattacks, review existing statute, and make recommendations to improve the state's cybersecurity.	Governor, Lieutenant Governor, Speaker of the House, standing committees of primary jurisdiction over state government operations	Continue
4. Data Center Services Consolidation Measurement Report	Section 2054.062, Texas Government Code	Requires DIR to annually report an evaluation of actual costs and cost savings related to an IT consolidation initiative, including whether the project is on time.	Legislative Budget Board, DIR board, customers involved in consolidation	Continue
5. Biennial Consolidated Assessment of Agency IT Infrastructure	Section 2054.068, Texas Government Code	Requires DIR to biennially report an analysis and assessment of state agencies' security and operational risks and, for high-risk agencies, a detailed analysis of agency efforts to address risks and related vulnerabilities.	Governor, Lieutenant Governor, Speaker of the House, chairs of the House Appropriations and Senate Finance committees, Legislative Budget Board	Continue
6. Prioritized Cybersecurity and Legacy Systems Report	Section 2054.069, Texas Government Code	Requires DIR to biennially prioritize, for the purpose of receiving funding, state agency cybersecurity projects and projects to modernize or replace legacy systems.	Legislative Budget Board	Continue

Appendix G

Report Title	Legal Authority	Description	Recipient	Sunset Evaluation
7. Report on the Placement of Information Resource Managers in Agency Hierarchies	Section 2054.075, Texas Government Code	Requires DIR to continually report the extent and results of state agencies' compliance with statute requiring that information resources managers report to the executive head or deputy executive head of an agency.	Legislature	Abolish - See Recommendation 5.2
8. State Strategic Plan for Information Resources Management	Sections 2054.091-2054.094, Texas Government Code	Requires DIR to collaboratively identify goals for all state agencies to follow when developing the information technology components of their agency strategic plan.	Governor, Legislative Budget Board	Modify - See Recommendation 5.2
9. Report Status of Information Resources Deployment Review Corrective Action Plans	Section 2054.097, Texas Government Code	Requires DIR to report as needed the status of corrective action plans DIR has required agencies to create to comply with the *State Strategic Plan for Information Resources Management*.	State Auditor's Office, Legislative Budget Board	Continue
10. Report on Non-Compliant Agencies	Section 2054.102(c), Texas Government Code	Requires DIR to continually update a list of agencies that have not complied with DIR standards, the *State Strategic Plan for Information Resources Management*, or corrective action plans related to information resources deployment.	Legislative Budget Board	Continue
11. Consolidated Information Security Report	Section 2054.133(f), Texas Government Code	Requires DIR to biennially report the state's information security maturity as measured against the state's Texas Cybersecurity Framework.	Governor, Lieutenant Governor, standing committees of primary jurisdiction over DIR's evaluation of information security	Continue
12. Report on Texas.gov	Section 2054.260, Texas Government Code	Requires DIR to biennially report on the status, progress, benefits, and efficiency gains through the state electronic internet portal, Texas.gov, and financial matters, including project costs and revenues and significant issues regarding contract performance.	Governor, Lieutenant Governor, Speaker of the House, committee chairs of primary jurisdiction over DIR, each state agency and local government participating in Texas.gov	Continue
13. Audit Report of the State Electronic Internet Portal	Section 2054.2721, Texas Government Code	Requires DIR to annually report the results of an independent annual audit of Texas.gov.	Governor, Lieutenant Governor, Speaker of the House, committee chairs with primary jurisdiction over DIR, each state agency and local government participating in Texas.gov	Continue

Appendix G

Report Title	Legal Authority	Description	Recipient	Sunset Evaluation
14. Report of the Disuse by a State Agency of a Statewide Technology Center	Section 2054.391, Texas Government Code	Requires DIR to report when it 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 with DIR.	Legislative Budget Board, Office of the Comptroller of Public Accounts, State Auditor's Office, the affected state agency	Continue
15. Report on the Consolidated Network Security System	Section 2059.057, Texas Government Code	Requires DIR to biennially report the accomplishments of the consolidated network security system's service objectives and performance measures, including financial performance.	Governor, Lieutenant Governor, Speaker of the House, State Auditor's Office	Continue
16. Report on the Use of Cloud Computing Services Options	Section 2157.007(e), Texas Government Code	Requires DIR to biennially report on the use of cloud computing services options by state agencies, including use cases that provided cost savings and other benefits, including security enhancements.	Governor, Lieutenant Governor, Speaker of the House	Continue

Appendix H | Staff Review Activities

During the review of the Department of Information Resources (DIR), Sunset staff engaged in the following activities that are standard to all Sunset reviews. Sunset staff worked extensively with agency personnel; attended board meetings; interviewed board members; met with staff from key legislative offices; conducted interviews and solicited written comments from interest groups and the public; reviewed agency documents and reports, state statutes, legislative reports, previous legislation, and literature; researched the organization and functions of similar state agencies in other states; and performed background and comparative research.

In addition, Sunset staff performed the following activities unique to this agency.

- Toured the state data centers in Austin and San Angelo, the Network Security Operations Center, and the Regional Security Operations Center in San Angelo.
- Toured the Network Operations Center in the Capitol Complex.
- Surveyed and interviewed DIR customers, including state agencies, institutions of higher education, local governments, and school districts.
- Interviewed DIR vendors.
- Attended meetings of numerous DIR committees and stakeholder groups, including the Artificial Intelligence Advisory Council, Artificial Intelligence Working Group, Customer Advisory Committee, Data Management Advisory Committee, Shared Technology Services governance groups, State Agency Coordinating Committee, Statewide Information Security Advisory Committee, and Texas Cybersecurity Council.
- Attended a Statewide Digital Accessibility Coffee Chat and Information Resources Deployment Review office hours session.
- Attended several DIR-sponsored events, including Artificial Intelligence Day, the Information Security Forum, and a government cybersecurity roadshow.
- Attended a cybersecurity webinar conducted by industry professionals.

Sunset Staff Review of the *Department of Information Resources*

REPORT PREPARED BY

Lauren Ames, *Project Manager*

Katherine Durain

Anthony Ellis

Annie Kuhl

Carl Perry III

Elizabeth Saenz

Emily Johnson, *Project Supervisor*

Eric Beverly
Executive Director

Sunset Advisory Commission

Location
Robert E. Johnson Bldg., 6th Floor
1501 North Congress Avenue
Austin, TX 78701

Mail
PO Box 13066
Austin, TX 78711

Website
www.sunset.texas.gov

Email
sunset@sunset.texas.gov

Phone
(512) 463-1300