ITI Promoting Innovation Worldwide

Texas Sunset Advisory Commission
PO Box 13066
Austin, Texas 7871

May 16, 2024

RE: Comments from the Information Technology Industry Council (ITI) regarding the Sunset Staff Report on the Department of Information Resources, as submitted to the Sunset Advisory Commission.

The Information Technology Industry Council (ITI) appreciates the opportunity to comment on the Texas Sunset Advisory Commission's Staff Report on the Department of Information Resources (DIR).

ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers with the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

ITI strongly supports DIR's goal to ensure state entities keep pace with advances in technology and deliver a more secure and optimized government experience for Texans. We are privileged to represent companies who provide the most innovative and secure technological solutions to all governments, and we remain committed to sharing the IT industry's perspectives as it relates to reviewing Texas' overall procurement and cybersecurity processes that impact the information and communication technology (ICT) industry.

ITI offers the following comments and recommendations regarding the Sunset Staff Report on the Department of Information Resources for consideration by the Texas Sunset Advisory Commission:

I. Issue 2 - DIR Could Improve Statewide IT Planning by Strengthening Its Reports to the Legislature and Expanding State Agency Procurement

Section 2.2 Require DIR to develop an IT procurement certification

ITI strongly supports the DIR developing and implementing a cross-functional IT procurement certification and related IT procurement training programs for government acquisition professionals. These initiatives will help ensure that government personnel understand the innovative technologies they are procuring. Specifically, the IT procurement certification should be developed in consultation with industry and periodically updated to ensure the certification requirements remain current and in line with commercial best practices. ITI recommends that this training program:

- include learning objectives related to market research, communicating with industry and industry perspectives on the procurement process, including how investment decisions are impacted by government communication and engagement, developing requirements, acquisition planning, best practices for developing and executing outcome-based contracts, and source selection strategy, evaluating proposals, and awarding and administering contracts for information and communications technology;

- include learning objectives that provide a basic understanding of key technologies state agencies need, such as cloud computing, artificial intelligence and artificial intelligence-enabled applications, and cybersecurity solutions;
- include learning objectives that encourage the use of commercial or commercially available off-the-shelf (COTS) technologies to the greatest extent practicable;
- include training on procuring technology through pricing models used for technology solutions used in the private sector, including the use of consumption-based pricing models for solutions procured on a subscription or tenancy basis (e.g., cloud solutions, data center services, software-as-a-service, etc.);
- include case studies of lessons learned from previous IT procurements and contracts;
- include experiential learning opportunities, and opportunities to practice acquisition teaming involving collaboration of team members with varied relevant domain expertise to complete acquisition-related tasks, including tasks with accelerated timelines;
- include continuous learning recommendations and resources to keep the skills of acquisition workforce members current, including tools that help adopt or adapt the use of innovative acquisition practices or other flexible business practices commonly used in commercial buys;
- be appropriately funded and made available to all relevant acquisition workforce members and program management personnel in the State; and
- inform agencies about streamlined and alternative procurement methods for procurement of commercial technology, including innovative procurement techniques designed to streamline the procurement process and lower barriers to entry.

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

ITI strongly supports the DIR developing an IT procurement training program for both front line acquisition professionals and agency executive leadership. By providing appropriate training at all levels of government and for all personnel involved in the IT procurement lifecycle, DIR will be contributing to a culture of innovation and cybersecurity within Texas state agencies. This program should be properly resourced to ensure it is effective, scalable, and sustainable over time.

The DIR should expand aspects of the IT procurement training program discussed above to focus on functions that are especially helpful for state executive leaders. The State’s leadership must have a keen understanding of the IT procurement process and cybersecurity risk management; therefore, executive training programming must focus on developing leaders that prioritize IT modernization and are able to develop and execute an enterprise IT modernization strategy. By empowering agency leaders to understand and implement innovative technologies, DIR will help ensure government leaders can use technological advancements to optimize their agencies’ missions.

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

ITI supports the recommendation that DIR develop a procurement-as-a-service pilot program, especially one that is focused on improving the delivery of shared IT services across the State and promoting the use of innovative procurement methods to acquire commercial technologies.

Similar programs have been used successfully in the federal government to help leverage procurement expertise and promote best practices across agencies. For example, the U.S. Department of Homeland Security (DHS) created its Procurement Innovation Lab (PIL) to provide procurement-related support to all DHS agencies. As described by DHS, the PIL is a "DHS framework aimed at experimenting with innovative acquisition techniques across the DHS enterprise. The PIL provides a safe space to test new ideas, share lessons learned, and promote best practices. It fosters cultural changes that promote innovation and managed risk-taking through a continuous feedback cycle."[1] By developing a centralized procurement office focused on innovation and providing technical assistance to other state agencies, the DIR can serve as a leader in driving procurement innovation across Texas.

ITI also recommends that DIR prioritize procurement resources toward providing shared services and/or enterprise contracts for cloud purchasing, cybersecurity monitoring, and other critical services. DIR could serve as the executive agent for statewide contracts, with individual state agencies being required to leverage approved solutions that are already centrally accredited through DIR cybersecurity processes. This would help reduce duplicative efforts and ensure all state agencies are leveraging approved and secure technologies to the maximum extent practicable.

II. Issue 3 - Adjustments to Two of DIR's Main Contracting Programs Could Better ensure the State Gets the Best Deal on IT

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

In addition to this recommendation that DIR periodically review COOP and other statewide contracts periodically for vendor pricing, ITI recommends that DIR focus on policies and practices that promote transparency, improve data-driven procurement decisions, and support supplier diversity through the DIR's technology acquisition process. Recommendations include the following:

- The DIR should standardize market research procedures, including requiring acquisition officials to conduct market research for commercial items and promoting transparency by requiring all market research opportunities to be posted on a single, public-facing DIR website.

- DIR acquisition officials should be required to provide original equipment manufacturer (OEM) subcontractors with access to relevant contract opportunity information (e.g., market research requests, requests for information (RFIs), and requests for proposals (RFPs)), rather than just providing these to prime contractor resellers. This will increase government transparency while also ensuring that the DIR has access to OEM expertise regarding innovative solutions and cost savings. The DIR should also be encouraged to consider adopting a requirement for

[1] https://www.dhs.gov/pil.

procurement of ICT from only OEMs or authorized resellers, as this will promote both transparency and supply chain visibility.

- DIR acquisition officials should be required to ensure, when conducting an evaluation of a proposal that intends to leverage goods or services through a separate enterprise service agreement or similar contract, that the total cost of ownership (including the cost or price of such goods or services under the separate agreement) is included in the evaluation of the proposal. This will address the concern within the IT industry that government agencies may avoid migrating away from less secure and less capable technologies in favor of modern, more capable, and more secure solutions based largely on the shorter-term costs of transitioning.

- The DIR should be required to adopt acquisition strategies, policies, and practices that promote competition, cost savings, and statewide cybersecurity through supplier and product diversity, including establishing a preference for multiple-award, solution-based categories and contracts over single-award, vendor-specific categories and contracts. The DIR should be required to closely monitor contract awards across state agencies and take the necessary steps to diversify the industrial base in areas necessary to perform mission-critical needs.

IV. Issue 4 - DIR Needs More Tools to Protect the State’s Cybersecurity

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

ITI supports requirements for state agencies to obtain a periodic DIR-selected information security assessment. Having DIR define the common baseline of security controls and best practices that are applicable to all state agencies will help reduce confusion and redundancy across state agencies, while also supporting agencies in improving their cybersecurity posture. Once a baseline of common controls is established, DIR should require periodic information security assessments against these common criteria, with the ability to measure agencies’ progress in meeting and exceeding controls over time.

ITI recognizes that the recently established U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC) Program[2] could offer a useful model and lessons learned for safeguarding government data and information systems while promoting standard procedures for periodic self and third-party cybersecurity assessments.

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

ITI supports this recommendation to modify information security assessment reporting requirements to ensure they do not duplicate or conflict with other required information in state agencies’ information security plans. Streamlining administrative reporting requirements will allow state agencies to devote more scarce resources to higher-value security tasks, such as facilitating continuous monitoring of networks and systems and responding to actual threats.

[2] https://dodcio.defense.gov/CMMC/Model/.

To further reduce duplicative efforts and ensure alignment with other government cybersecurity frameworks, such as those used by the U.S. federal government, ITI recommends DIR adopt the latest version of the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF). NIST breaks the CSF down into five core elements of an organization's cybersecurity strategy: identification, protection, detection, response, and recovery. Texas state agencies should consider the CSF as a roadmap to developing a strong cybersecurity infrastructure that provides the following functions:

- **Identification:** ITI recommends that DIR lead a statewide effort to identify and understand the full scope of risks to government functions, as well as developing a comprehensive inventory of available government security personnel and IT assets such as hardware and software. The DIR can play a major role in building shared situational awareness and a common operating picture among government personnel that will drive the eventual response strategy in the event of a cybersecurity incident. Building shared situational awareness is primarily a human issue, rather than a machine-driven function. The DIR should devote time to communicating and educating staff across state agencies about the relevant threat landscape, as well as providing staff with tools to gather real-time information that will help make predictions about potential future security events.

- **Protection:** Once the threat landscape is understood, the DIR should lead the development of a statewide strategy to establish safeguards to ensure that critical infrastructure services remain operational even during a cyberattack and to limit the potential impact of attacks. Personnel across state agencies should be well trained in threat awareness and mitigation strategies, and this training should be periodically evaluated through tools such as penetration testing and tabletop exercises. Commercial managed cybersecurity service providers should be strategically leveraged to supplement government resources by providing everything from continuous threat monitoring and intelligence to incident response and recovery.

- **Detection:** The best strategy for limiting the potential impact of a cyberattack is early detection. The DIR should encourage all state agencies to implement a continuous monitoring capability to monitor cyberthreats. Continuous monitoring processes must be reevaluated and updated frequently to incorporate the latest threat intelligence that could lead to cyberattacks. To that end, regular government engagement with private sector partners is critical.

- **Response:** Whenever a cybersecurity incident is detected, DIR should ensure state agencies quickly deploy a pre-determined response plan that includes all relevant stakeholders. The DIR should continue playing a critical role in developing, executing, and updating a whole-of-state cybersecurity incident response plan, including serving as a focal point for coordinating with other state and/or federal law enforcement officers and agencies.

- **Recovery:** Following a cybersecurity incident and execution of a statewide cybersecurity incident response plan, the DIR should oversee the restoration of government capabilities and citizen services as soon as possible. The DIR should work with all state agencies to develop a recovery plan that focuses on standard processes and timeframes for restoring systems, assets, and access to services. It is important to develop and deploy a comprehensive communications plan to all internal and external stakeholders to share recovery updates—DIR can greatly assist with ensuring consistent, accurate, and timely communications across the State. Finally, DIR should lead efforts to update the recovery plan to ensure future recovery efforts incorporate improvements and lessons learned.

V. ITI General Recommendations

In addition to our responses to the Sunset Staff Report, ITI offers the following general recommendations to be considered in DIR's sunset review:

Promote the adoption of commercial terms and conditions. The State of Texas benefits greatly from using commercial and COTS products, services, and solutions. By purchasing with substantially the same terms and conditions as those offered to the commercial marketplace, the State can leverage best-in-class technologies powered by private sector innovation. In contrast, government-specific terms and conditions can limit functionality, drive up cost, and potentially reduce the State's access to commercial offerings. We encourage the DIR to promote commercial and COTS solutions to the greatest extent practicable across the Texas State Government, while limiting the application of government-unique terms and conditions. DIR should consider incorporating the following best practices in state contract terms and conditions:

- **Limitation of Liability:** When considering terms and conditions for IT products, it is critical for the limitation of liability to reflect the variety of today's IT solutions and service models. ITI encourages including separate liability caps to address the substantive differences between maintenance or subscription-based services, implementation or project-based services, and staff augmentation support or training/management services. Liability must also be treated as more of a "shared responsibility" model between the State and industry. A shared model of liability would help right-size risks and ensure the State's continued access to innovative commercial technologies.

- **Protecting Intellectual Property (IP):** It is vitally important that state IT contracts include appropriate protections for contractors' intellectual property and other proprietary or sensitive data. This is especially important for contracts for commercial solutions that incorporate technologies developed solely at private expense. The DIR must encourage statewide contract terms and conditions to include commercially standard IP protections for government suppliers. Additionally, the DIR should ensure standard commercial terms and conditions apply to limit the State's right to disclose potentially sensitive IP to third parties and to authorize recipients to use, modify, reproduce, perform, release, display, create derivative works from, and disclose such IP for any State government purpose.

Empower Texas state agencies for long-term cyber resilience. Cybersecurity is an ongoing process that requires constant monitoring and adaptation. As technology evolves and threat actors adjust their techniques, the DIR is uniquely positioned to embolden Texas state agencies' commitment to good cybersecurity hygiene. This includes dedicating sufficient funding, adopting cutting-edge commercial technologies, and supporting long-term workforce expertise. It is also critical for the DIR to promote a risk-based cybersecurity approach that is aligned with commercial best practices and does not duplicate or conflict with existing applicable cybersecurity requirements and standards at the U.S. Federal Government level. To facilitate alignment with commercial best practices, we urge the DIR to survey the market—especially the OEM community—to ensure a robust understanding of industry standard security practices. With the DIR's support in setting long-term and adaptive cybersecurity best practices, Texas state entities can maintain their systems while collaborating closely with industry partners to ensure their cybersecurity posture remains current and effective.

Promote longstanding acquisition policies that leverage the benefits of global supply chains. As the Texas Government navigates an ever-evolving technological landscape, it faces a multitude of risks in safeguarding the State's ICT supply chain. Malicious actors may try to use the ICT supply chain to harm vital national interests, impact the timely delivery of government services, or degrade an agency's operations and mission, to mention only a few possible effects. It is crucial that the DIR works closely with private industry—including promoting the sharing of relevant threat information between the public and private sectors—to support adoption of a risk-based approach for securing the Texas Government's ICT supply chain.

ITI encourages the DIR to leverage the NIST Risk Management Framework when developing threat monitoring and mitigation measures.[3] This comprehensive and flexible framework aims to address supply chain threats through actions that consider the nature and context of the equipment and are appropriately tailored to balance the risk with the consequences of the mitigating action. Adopting a targeted risk-based approach—rather than a one-size-fits-all solution that focuses on a single or small number of risk factors—is crucial for ensuring the DIR can help address statewide ICT supply chain risks while maintaining access to top-tier commercial solutions that meet the needs of Texans.

Workforce development and support. Fostering technological expertise and building a skilled workforce throughout the Texas Government is pivotal for harnessing the transformative potential of innovative technologies, including but not limited to artificial intelligence (AI) and cybersecurity innovations. To ensure Texas is best positioned to optimize the benefits of these commercial technologies, it is important to build a skilled acquisition and technical workforce that understands new tools and services. This includes training employees in technical concepts, tools, and ethics, as well as advancing and incentivizing professional and technical apprenticeships, education, and training programs. Increasing resources for hiring, training, and retaining your acquisition and technological workforce is important, but building a sustainable pipeline of talent with diverse backgrounds and perspectives is essential for driving long-term mission outcomes. This will not only enhance the efficiency and effectiveness of governance but also foster greater trust and confidence among constituents.

This need for a skilled workforce is further underscored by the increasing volume of IT requirements by the Texas Government and the growing statutory and audit requirements for public procurement processes. As the demand for IT products and services from state agencies and local government entities becomes increasingly challenging to meet, additional Full Time Employees (FTEs) assigned to the DIR are essential. Without additional FTEs, the DIR will have to scale back its offerings, potentially

[3] https://csrc.nist.gov/projects/risk-management/about-rmf.

hampering the ability of state entities to effectively serve Texans and provide proper oversight and compliance. Implementing strong workforce development and support strategies will enable the DIR to build a robust and agile workforce capable of enhancing technological capabilities across Texas agencies and improving the delivery of constituent services.

VI. Conclusion

ITI appreciates your consideration of our recommendations and looks forward to any additional opportunities for industry participation in this important process. Should you need more information or wish to discuss our recommendations, please contact me at kgaudette@itic.org.

Very Respectfully,

Kelsey Gaudette

Kelsey Gaudette
Manager, Public Sector State and Local Policy
Information Technology Industry Council (ITI)