Transforming How Texas Government Serves Texans

An Overview of Regional Security Operations Centers in Texas

Texas Department of Information Resources
Office of the Chief Information Security Officer

December 2023

Table of Contents

Executive Summary

The Texas Department of Information Resources (DIR) established the state's first regional security operations center (RSOC) in 2022 in partnership with Angelo State University. By choosing public institutions of higher education (IHEs) to host RSOCs, Texas can help secure local government entities such as cities, counties, and independent school districts (ISDs) from cyber threat actors while concurrently increasing the quality and quantity of cybersecurity analysts in Texas. This white paper outlines how and why Texas established the pilot RSOC at Angelo State University. DIR wrote this white paper to guide agencies and other organizations outside of Texas who are interested in implementing a similar program.

Background

The Problem

DIR observed the need for RSOCs after the August 2019 statewide ransomware incident that simultaneously impacted 23 local government entities. Texas Governor Greg Abbott declared this never-before-seen incident a state disaster event, a first for cybersecurity, and activated the Texas State Operations Center for resolution. The widespread impact of the August 2019 incident necessitated the activation of additional statewide resources, including the Statewide Incident Response Workgroup.[1]

The August 2019 incident, a focusing event for DIR and many other Texas state agencies, highlighted how vulnerable many local government entities are to cybersecurity incidents. DIR sought to use the lessons from the August 2019 incident as impetus to effect positive change for Texas, remedying this statewide vulnerability and strengthening local government entities' security posture through cybersecurity support and training provided through the RSOCs.

In the last five years, DIR has fielded reports of 163 ransomware incidents impacting Texas entities (as of the publication date of this white paper).

Of ransomware incidents reported to—or discovered by—DIR, approximately 90 percent targeted local government entities such as counties, cities, and ISDs. The growing number of ransomware incidents impacting Texas local government entities indicates that cybersecurity at the local level needs strengthening.

[1] The Statewide Incident Response Workgroup, led by DIR, is a collaboration between state agencies, federal law enforcement, and private sector partners to plan and exercise the state's response to a significant cybersecurity incident.

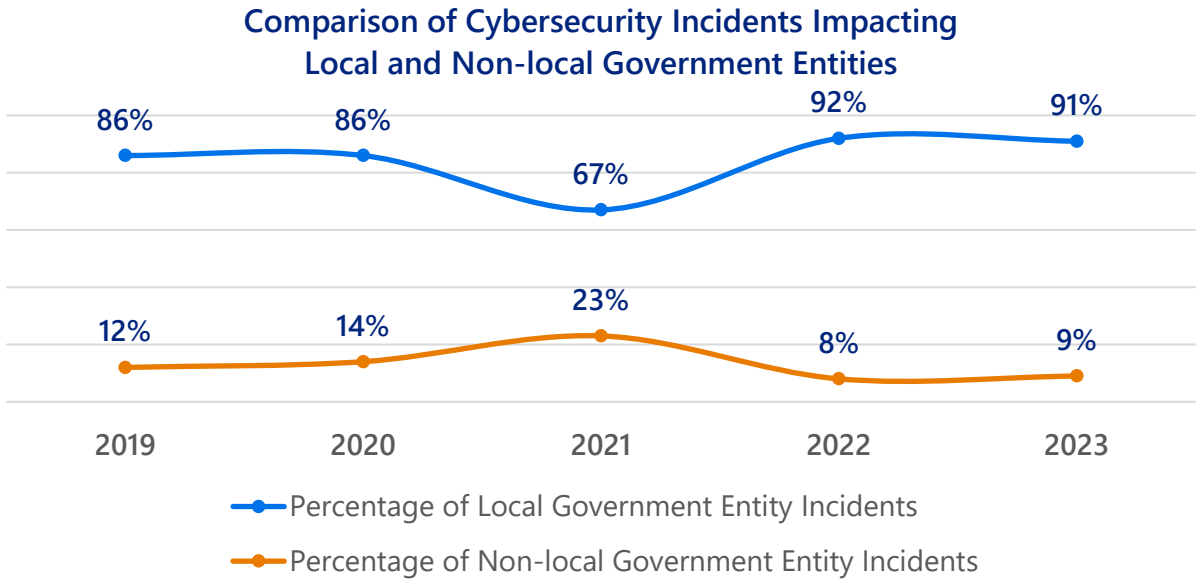

Figure 1 | Comparison of Cybersecurity Incidents Impacting Local and Non-local Government Entities

The Solution

The August 2019 event demonstrated that local government entities in Texas needed additional cybersecurity training, resources, and incident response tools. To help, DIR proposed creating security operations centers across Texas, dedicating a designated Cybersecurity Incident Response Team (CIRT) at DIR, and forming a Volunteer Incident Response Team (VIRT) to activate in case of another statewide cybersecurity disaster.

On November 15, 2020, DIR published the 2020 Cybersecurity Report[2] outlining these recommendations. (Government Code 2054.0591 requires DIR to provide legislative recommendations for improving the state's cybersecurity posture and protecting against cybersecurity incidents.)[3] The Texas Legislature codified many of these recommendations in Senate Bill 475 during the 87th Legislative Session, effective September 1, 2021.[4] Furthermore, the Texas Legislature affirmed its support of these initiatives by granting DIR additional full-time employees and general revenue funding.

In December 2021, DIR posted the Regional Security Operation Center Expression of Interest Overview, inviting all interested public IHEs to submit proposals explaining why their institutions should be selected as the pilot RSOC.[5] Per Government Code 2059.203, private IHEs were not eligible for selection as the pilot RSOC.[6]

In April 2022, DIR chose to partner with Angelo State University to host the pilot RSOC; by July 2022, all agreements and contracts were finalized. As the RSOC host, Angelo State University was chosen to operate the RSOC on behalf of DIR.

[2] 2020 Cybersecurity Report
[3] Gov't Code § 2054.0591
[4] Texas Senate Bill 475
[5] Regional Security Operation Center Expression of Interest Overview
[6] Gov't Code § 2059.203

From July to December 2022, DIR and Angelo State University worked together to establish the pilot RSOC. During this time, DIR granted Angelo State University flexibility in acquiring—or utilizing existing—technology solutions that made sense for its security operations.

DIR's future vision is to secure Texas with an RSOC in each of the twelve economic regions established by the Texas Comptroller, depending on approval from the Texas Legislature. Each of the twelve economic regions in Texas contains at least one IHE. Hosting RSOCs in IHEs in each economic region ensures that all of Texas could eventually be under the protection of an RSOC.

As of the publication date of this white paper, DIR has established one functioning RSOC (Angelo State University) and has received funding from the Legislature for two additional RSOCs (University of Texas at Austin and University of Texas Rio Grande Valley).

Timeline of Events

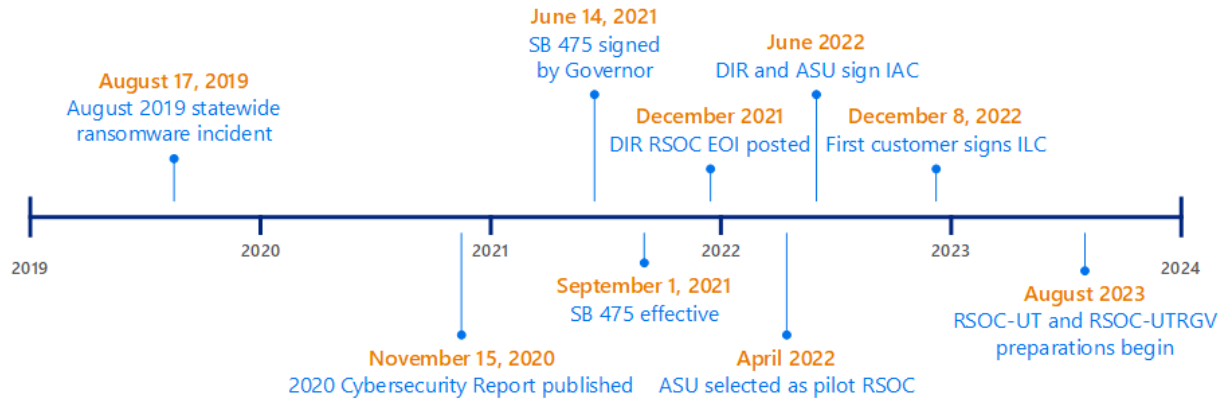

Figure 2 | Timeline of Events

How the Pilot RSOC in Texas Operates

In simple terms, an RSOC is a cybersecurity command center that monitors, collects, and analyzes data related to mitigating cybersecurity incidents for affiliated entities in a defined region. RSOCs proactively monitor affiliated entity servers, systems, infrastructure, and endpoints for signs of suspicious activity that may indicate the presence of a cyber threat actor. If suspicious activity is confirmed, the RSOC can step in to provide service and help resolve the incident.

Table 1 | RSOC Services outlines the services available to affiliated entities of an RSOC.

RSOC Services				
Real-time security monitoring	Security alerts and guidance	Immediate response	Policy and planning	Cyber education and awareness

Table 1 | RSOC Services

To join, interested entities must first contact their region's RSOC to inquire about eligibility. If deemed eligible, the entity and RSOC will enter into an interlocal contract that defines the partnership. Once the interlocal contract has been signed, the RSOC will onboard the entity and

begin providing RSOC services. (Before offering service to eligible entities, the RSOC must enter into an interagency contract with DIR.)

Table 2 | Entities Eligible for RSOC Services outlines the seven classifications of entities that are eligible for RSOC services.

Entities Eligible for RSOC Services			
Cities	Counties	Independent school districts	Public junior colleges
Special districts	State agencies	Independent organizations as defined by Utilities Code Section 39.151(b)[7]	

Table 2 | Entities Eligible for RSOC Services

RSOC services are free for all eligible entities. DIR receives funding for the RSOCs from the Texas Legislature.

RSOCs provide the greatest benefit when partnerships are established before an affiliated entity has a cybersecurity incident; however, an unaffiliated entity experiencing a cybersecurity incident can receive support from an RSOC at DIR's instruction and on behalf of DIR.

The value of Texas' region-based approach to cybersecurity is two-part:

- RSOCs can more easily establish and maintain relationships with entities that are **geographically nearby**.
- RSOCs can serve **smaller, underserved entities** that otherwise have minimal resources at their disposal.

Geographically Nearby and Poised for Activation

As a major driver of culture, geography plays a significant role in shaping the expectations for what a region considers normal and acceptable when establishing trust and accepting help. Though only a single state, Texas contains a multitude of cultures, attitudes, values, and customs that are often linked to the different regions of the state.

Texas is also, of course, geographically significant. The sheer size of Texas necessitates delegation of resources to an entity within a manageable time frame from an impacted entity.

Figure 3 | Entities Eligible for RSOC Services

[7] Utilities Code § 39.151(b)

Establishing Trustworthy Partnerships

Trust is complicated enough without the added stress of dealing with a cybersecurity incident. People who exist in the same spaces, however, are more likely to trust and accept help from others who they view as similar[8] in the event of a cybersecurity incident.

While establishing security operations centers (SOCs) on an even more granular level would further bridge this division between trust and security, factors such as cost, time, and overall effort prohibit this from feasibility. RSOCs, therefore, provide a happy medium between facile establishment of trust and timely allocation of quality cybersecurity resources.

In a field where caution is paramount, quickly establishing trust with an assisting or supporting agency during a cybersecurity incident—or better yet, having that relationship defined before the incident occurs—is critical[9]. When DIR responds to incidents after notification from an unaffiliated third party, valuable time is often spent convincing impacted entities of DIR's identity and genuine commitment to helping resolve the incident. Having an RSOC that acts on behalf of DIR in such situations ensures that the scope of DIR resources and knowledge is administered with the more personalized touch of a well-known, local entity.

Shortening Response Times

If resources are required onsite for an affiliated entity, RSOC personnel are nearby to provide timely assistance. In a state as expansive as Texas, quick allocation of resources can be the difference between quick containment and extensive recovery efforts. Additionally, the staff employed at the RSOCs are more likely to have in-depth, local knowledge about an impacted entity, which allows them to make decisions related to the entity's protection quicker than a centralized, generalized entity such as DIR.

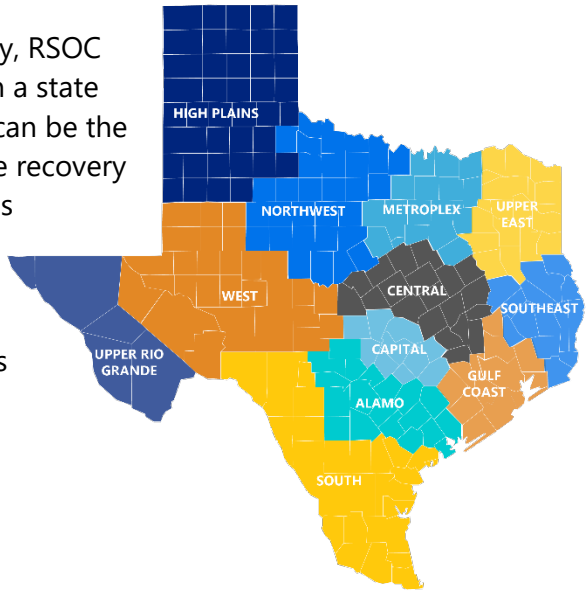

Figure 4 | Economic Regions in Texas

Serving the Underserved

In recent years, DIR has observed an increasing number of cybersecurity incidents impacting entities such as small local governments.[10] Smaller entities often face challenges related to aging infrastructure, lack of qualified security personnel, and strict budgets that leave their information assets vulnerable. DIR seeks to address these shortcomings by bringing high-budget resources to entities with low budgets. By affiliating with an RSOC, smaller entities get access to cybersecurity resources that would otherwise be unavailable to them.

[8] Societal Trust and Geography
[9] Broken promises: How trust affects cybersecurity
[10] 2022 Cybersecurity Report

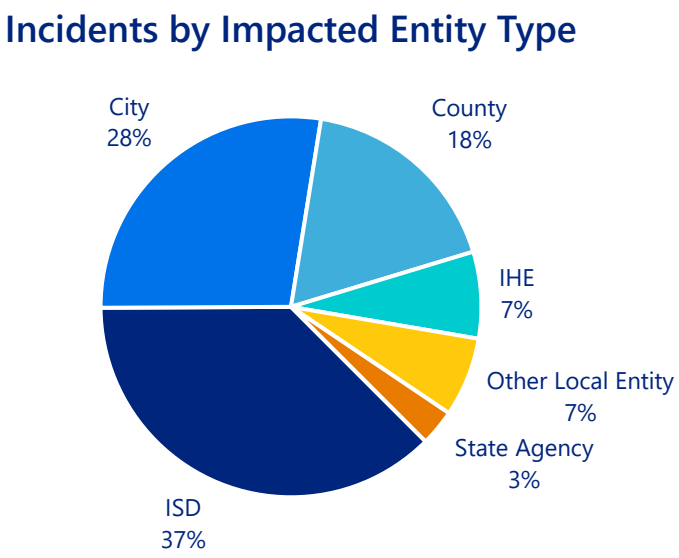

Figure 5 | Incidents by Impacted Entity Type

Local government entities are not required to follow state security standards; however, by encouraging local government entities to join an RSOC, DIR ensures that local government entities receive a baseline of cybersecurity protection, and at no cost to them.

Why the Pilot RSOC Has Been Successful

DIR chose to partner with Angelo State University as host of the pilot RSOC due to its impressive expression of interest, which clearly outlined how the university would ensure success for the pilot RSOC. In its expression of interest, Angelo State University identified both short- and long-term goals that directly aligned with DIR's plans for the pilot RSOC.

As of the publication date of this white paper, 36 eligible entities have expressed interest in joining the pilot RSOC at Angelo State University in the West economic region. Of those 36 eligible entities, 18 have signed an interlocal contract for RSOC services.

Angelo State University has ensured the continued success of Texas' pilot RSOC through three key factors:

- Securing **executive buy-in** from all levels of the chain of command, but most importantly from high up the chain.
- Leveraging—and stressing the importance of—**existing relationships**.
- Utilizing **existing infrastructure and capabilities**.

Executive Buy-in from All Levels of the Chain of Command

Before even sending in their expression of interest, Angelo State University's leadership understood the importance of cybersecurity. Prior to being selected as one of the university's highest-ranking officials, the current president of Angelo State University, retired U.S. Air Force Lieutenant General Ronnie Hawkins, was the Director of the Defense Information Systems Agency (DISA). Because of his experience, all levels of the chain of command at Angelo State University understood the significance of being selected as the pilot RSOC by DIR. In addition, the Provost and Vice President of Academic Affairs, Dr. Donald Topliff, has been active in, vocal

about, and engaged with personally overseeing the pilot RSOC instead of delegating to someone in his chain of command.

Having leadership that intimately knew and understood exactly what they would be asked to do as Texas' pilot RSOC was instrumental in its eventual success.

The Importance of Existing Relationships

Angelo State University brings a vast network of working and personal relationships to leverage when implementing and functioning as the pilot RSOC. Throughout the West economic region, Angelo State University has technological, academic, and interpersonal relationships with ISDs, junior colleges, private organizations, and more that can be leveraged as necessary. IHEs and ISDs often have working relationships due to their shared industry and purpose.[11] These relationships are advantageous for Texas, in part because they can be leveraged to onboard ISDs more easily into the RSOCs. For example, Angelo State University recently hosted Cybersecurity Camp for middle and high school students in the region to increase student interest in cybersecurity; both student analysts and RSOC staff collaborated to provide instruction and oversight of the camp.

Existing relationships are paramount when developing trust, onboarding eligible entities, and responding to cybersecurity incidents in the West economic region.

Existing Infrastructure and Capabilities

Having developed and matured the university's security program, Angelo State University had experience managing security information and event management (SIEM) tools, monitoring endpoints, and responding to cybersecurity incidents. Prior to submitting their expression of interest, Angelo State University analyzed its existing infrastructure—including backup generators, fiber lines, electric lines, buildings, and physical space—and realized that it could fulfill DIR's requests for the pilot RSOC.

Angelo State University's experience supporting large IT programs allowed them insight into comprehending the challenges and opportunities of expanding to include vulnerable entities in the region. As more entities join the RSOC and current infrastructure grows, the pilot RSOC gains a clearer, more comprehensive image of cybersecurity in the West economic region.

Student Analyst Success Story

Angelo State University has shared with DIR several success stories regarding student analysts working at the pilot RSOC. To date, student analysts working at the pilot RSOC have completed over 10,500 learning hours of cybersecurity training, preparing the next generation of Texas' cybersecurity analysts for full-time employment.

In addition to student analysts who went on to find full-time employment in the cybersecurity industry, DIR wants to highlight the success of a non-traditional student analyst who currently works in the RSOC (at the time of this white paper's publication).

Prior to pursuing secondary education at Angelo State University, this non-traditional student retired from working in the physical security sector. He decided to go back to school for his bachelor's degree, and, upon learning about the RSOC, decided to investigate whether his

[11] Collaborating with Local Schools

physical security proficiencies would translate to the cybersecurity sector. They did, and he now loves being a student analyst and is currently persuading his son to attend Angelo State University to follow in his footsteps. Thanks to the pilot RSOC, Texas will soon have another qualified cybersecurity analyst (and in time a steady stream of cybersecurity analysts) defending the state's digital assets.

Texas' Need for Skilled Cybersecurity Analysts

Like the nation, Texas has been impacted by the shortage of skilled cybersecurity analysts exacerbated by the COVID-19 pandemic.[12] Now that remote work has become more prevalent than ever before, cyber threat actors are proportionately—if not moreso—active.[13] The Federal Cyber Workforce Management and Coordinating Working Group, a 24-agency federal coalition headed by the Cybersecurity and Infrastructure Security Agency (CISA), recommends that the public sector counteract this shortage, in part by designing recruitment and development programs that focus on entry-level and non-traditional talent pools.[14]

The Legislature has decided to combat Texas' shortage of skilled cybersecurity analysts by hosting the RSOCs in IHEs for one primary reason:

- IHEs can employ college students to provide **valuable hands-on experience to the next generation of cybersecurity analysts** while offsetting RSOC staffing costs.

Hands-on Experience for the Next Generation of Cybersecurity Analyst

By hosting RSOCs in IHEs, the number and quality of graduates who expand into Texas' cybersecurity industry is likely to increase.

The skills gap between graduation and entry-level requirements can be hard to overcome for new graduates.[15] Many entry-level cybersecurity roles require applicants to have at least a year of experience to be considered for the position.[16] Due to the high stakes in cybersecurity, new graduates must be high caliber.

While working in an RSOC, student analysts gain valuable insight into how a SOC functions and what a role on a cybersecurity team entails. Working under trained cybersecurity analysts, student analysts realize real-world cybersecurity skills such as system monitoring, vulnerability management, threat hunting, and incident response in a secure environment. This valuable experience improves their resume and chance of gaining employment after graduating, while subsequently reinforcing the cybersecurity workforce.

More than half of college graduates plan on finding a job close to where they finish college.[17] DIR hopes that student analysts will remain in the region of the RSOC after graduating, bolstering the local cybersecurity workforce and creating a cybersecurity analyst job pipeline: ideally, the next generation of cybersecurity analyst starts their education in an RSOC-secured ISD, stays in the region for secondary education at the RSOC-hosted IHE, and graduates back

[12] Impact of COVID-19 on Cybersecurity
[13] A deeper look into cybersecurity issues in the wake of Covid-19: A survey
[14] State of the Federal Cyber Workforce: a Call for Collective Action
[15] Exploring the Gap between College and Career
[16] Guide to Entry-Level Cybersecurity Job Requirements
[17] Where do students want to live after graduation?

into the cybersecurity industry in the region, augmenting the system from which they benefited. Additionally, student analysts that worked in the RSOC graduate with experience working with—and for—government, an added bonus for DIR, other Texas state agencies, and local Texas governments.

Furthermore, staffing the RSOC with student analysts lowers staffing costs while ensuring that hard-to-fill shifts, such as the overnight shift, have coverage.

Considerations for Establishing RSOCs in Your State

This white paper is directed at regulatory information security agencies and other organizations interested in establishing a pilot RSOC in their states. However, anyone considering establishing a pilot RSOC (or a similar program) may find this white paper helpful.

Aside from the usual logistical considerations for implementing a SOC, your agency should consider:

- How you will **regionalize** your state.
- Where your pilot RSOC will be **located**.
- Who will **host** your RSOCs.
- What **student analyst training criteria and metrics** will look like.

Regionalize Your State

After determining the logistics of your pilot RSOC, you should decide what metrics or criteria to use to regionalize your state. Your state likely has existing maps of different regions, districts, or locales that you can use; however, you are not tied to using a pre-existing—or even geographical—map. Smaller states may consider regionalization in ways that are not strictly geographical; however, larger states should strongly consider geographic regions that focus on shortening response time for potential onsite incidents.

Consider an Underserved Region for Your Pilot RSOC Location

For your pilot RSOC, you should consider selecting an underserved region of your state that is vulnerable to cybersecurity incidents. By selecting an underserved region, you can capture key before and after metrics that clearly demonstrate the value and success of the pilot RSOC while simultaneously serving the most vulnerable area of your state.

Decide Who Will Host the RSOCs

Identifying who will host your RSOCs is closely linked to how you regionalize your state. You should consider hosts that maintain adequate coverage of your state while also balancing other aspects such as student analyst training.

You don't necessarily need to host your RSOCs in one type of organization; however, hosting RSOCs in one type of organization (such as IHEs) does add structure and consistency that your state's leadership may appreciate. Moreover, you can save time and resources by selecting RSOC hosts that already have a functioning SOC in place.

You should strongly consider hosts that have an increased capacity to train and instruct student analysts in a significant way. While IHEs may seem the natural choice, not all states have the same infrastructure or education systems to support their RSOCs.

Identify Student Analyst Training Criteria and Metrics

While not a mandatory part of an RSOC, including student analysts allows your agency to counteract the shortage of the nation's cybersecurity analysts while simultaneously increasing your state's current cybersecurity posture.

Working in an RSOC is beneficial to both the state and the students. Structuring your RSOCs to highlight the benefit of working in one ensures that interest stays high among the intended student populace. You may consider offering university credit, a certificate, or some other type of attractive compensation to students who take part in the RSOC.

If you are not interested in college students working in your pilot RSOC, you may consider a trainee, intern, apprentice, or similar program that taps into other unrealized, non-traditional sources of future cybersecurity analysts.

Conclusion

Texas has improved the state's cybersecurity posture by establishing a pilot RSOC in its West economic region. Texas' region-based approach to RSOCs allows for quick establishment of both trust and onsite resources in the event of a cybersecurity incident. By hosting the pilot RSOC in a public IHE (Angelo State University), Texas can concurrently improve the quality and quantity of Texas' cybersecurity analysts by employing and training student analysts in the RSOC.

Contact Us

If you are an interested eligible entity in or around the West economic region, contact Angelo State University via email at RSOC@angelo.edu for information on how to take advantage of no-cost, around-the-clock security monitoring, comprehensive threat hunting, advanced data analytics, and more.

For more information on Texas' RSOCs, email DIR's Office of the Chief Information Security Officer at CIRT@dir.texas.gov.

List of Tables and Figures