State

Texas

Agency

Texas Department of Information Resources

Award Category

Cybersecurity

Project Title

Whole of State in the Lone Star State

The Texas Regional Security Operations Centers 2.0

Project Dates

August 2023 – November 2024

Contact

Tony Sauerhoff
State of Texas Chief Information Security Officer
Tony.Sauerhoff@dir.texas.gov

Executive Summary

In 2021, the Texas Legislature passed Senate Bill 475, which created regional security operation centers (RSOCs) to provide "boots on the ground" support close to local governments that need assistance with major cybersecurity incidents. In 2022, the Texas Department of Information Resources (DIR) partnered with Angelo State University (ASU) in West Texas to operate the pilot RSOC and provide regional cybersecurity support to local governments and other eligible government entities, including K-12. Based on the success of this pilot partnership, DIR partnered with two additional institutions of higher education in November 2024: the University of Texas at Austin (UT) and the University of Texas Rio Grande Valley (UTRGV) for a second phase of RSOCs to cover additional regions of the state.

The first of their kind in the nation, the RSOCs offer security monitoring, alerting, guidance, training, and protection to help local governments prevent and recover rapidly from cybersecurity incidents. University students can work at the RSOC and receive hands-on experience, strengthening the cybersecurity workforce of tomorrow.

Idea

What problem or opportunity does the project address?

Increasing Sophistication of Cyber Threats

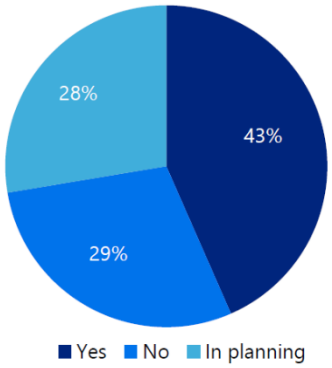
As cyber threats to public entities continually increase, government entities in all regions of the state need to be protected against attacks that can disrupt the delivery of services or compromise Texans' information. Ransomware incidents can greatly impact Texas government organizations, and 90 percent of known incidents occur at the local level. The number of ransomware incidents targeting counties, cities, and school districts indicates that cybersecurity programs at the local level need strengthening.

Limited Cybersecurity Resources

Additionally, cybersecurity workforce challenges continue to impact the cybersecurity risk landscape. At Texas state agencies, the number of agency cybersecurity personnel has not been keeping pace with the growing demand for cybersecurity expertise or resources, causing organizations to do more with less resources.

In 2024, agencies in Texas reported an increased focus on information technology (IT) security operations, but most agencies report that they do not have adequate resources budgeted to respond effectively to a major cybersecurity incident.

Percent of State Agencies with Adequate Resources Budgeted for Cybersecurity Incidents



Source: Texas Department of Information Resources, 2024 Cybersecurity Report

Why does it matter?

The state of Texas is an intriguing target for malicious actors due to the large number of public-sector information assets that house sensitive and confidential information. Over 200 state organizations and thousands of local governments organizations make Texas a target-rich environment for threat actors. To compound the issue, government entities must balance competing priorities and resources, which can create challenges in sufficiently preparing to address the impacts of cybersecurity incidents.

Over the last two years, Texas has faced its own cyber challenges affecting both the public and private sector, such as ransomware attacks and recent nation-state cyber threats. During this time, when new vulnerabilities are becoming more complex and frequent, security and risk management leaders have had to focus on balancing adequate protection and business growth.

What change will it make for Texans?

The RSOC model aims to meet these challenges across the state through collaboration between the state and public universities. Through the operation of RSOCs, DIR relies on its partnership with universities to strengthen the cybersecurity capabilities of today and the cybersecurity workforce of tomorrow. The RSOCs offer network security infrastructure that local governments can utilize in addition to providing real-time network security monitoring, network security alerts, incident response, and cybersecurity educational services.

The RSOCs play a crucial role in responding effectively and quickly to geographically distant or dispersed incidents. The RSOCs offer participating entities the following security services:

Real-Time Network Security Monitoring

to detect and respond to network security events that may jeopardize participating organizations and the residents of this state.

Alerts and Guidance

for defeating security threats.

Immediate Response

to detect and respond to network security events that may jeopardize participating organizations and the residents of this state.

Policy and Planning

to provide guidance on cybersecurity policies and plans to improve the cybersecurity posture of RSOC participants.

Cybersecurity Educational and Awareness Services

to assist participating organizations in establishing and strengthening sound security practices, including developing model policies, and planning to assist participating organizations in maturing their cybersecurity posture.

RSOCs enable organizations to respond effectively and quickly to geographically distant or dispersed incidents by centralizing incident management on a manageable regional scale to leverage remote investigation and analysis capabilities, coordinate response efforts, optimize resources, standardize processes, leverage technology, and foster continuous improvement. These capabilities collectively enhance incident response efficiency and minimize the impact of incidents across multiple locations.

What makes it different?

The vision driving the RSOC model aligns with a whole-of-state approach to cybersecurity that increases the threat protection and cyber maturity of all of Texas through collaboration and partnerships.

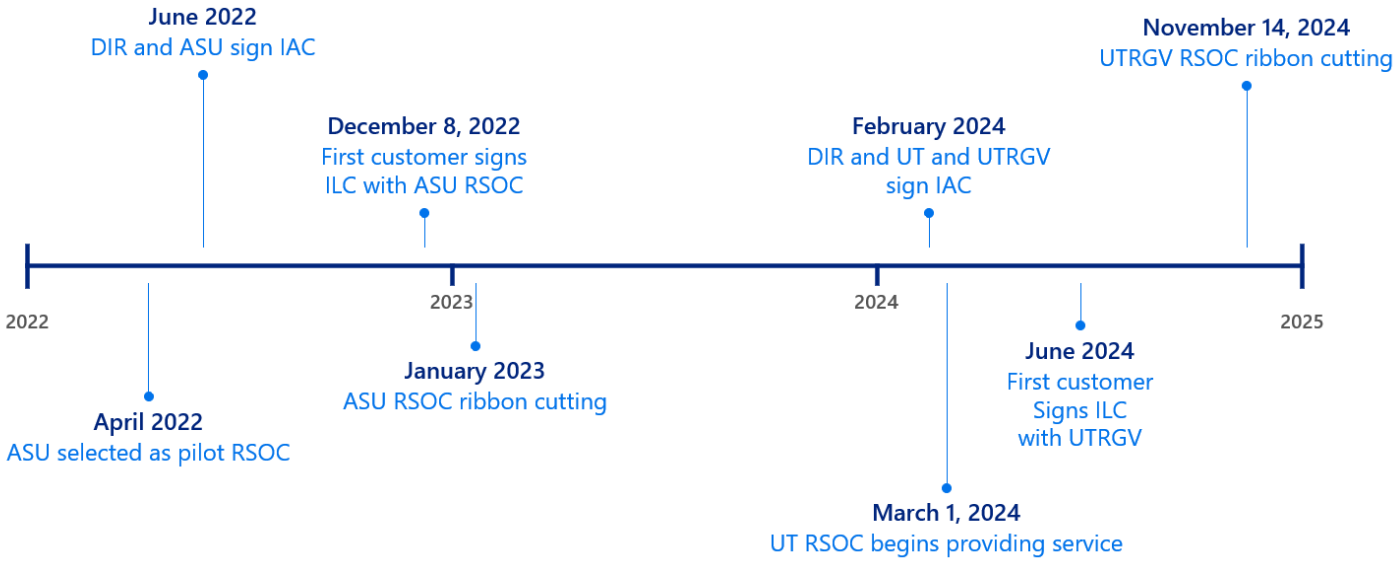
RSOCs provide "boots on the ground" support that is close in proximity to local governments that need assistance with major cybersecurity incidents. In operating this next phase of RSOCs, the UT and UTRGV RSOCs provide free security services to governmental agencies in the central, west, and south regions of Texas. The RSOCs are also training up a continuous pipeline of quality cybersecurity students to augment the RSOC while they gain real-world experience in offensive and defensive cybersecurity operations and intel support.

What makes it universal?

Texas' strategy with the RSOCs exemplifies the 2025 NASCIO State CIO Top Ten Priorities of **Cybersecurity and Risk Management** and **Workforce**. Cybersecurity risks are complex and may occur during other disruptions. As a result, there is an increasing need for regional responses and integrated continuity planning. Additionally, a *nationwide* shortage of skilled cybersecurity professionals continues to hinder the public sector's ability to recruit and retain staff with specialized skills. The RSOCs address those challenges with sustainable cybersecurity resources to meet security needs, including long-term investment in cybersecurity tools, talent, and training.

Implementation

What was the roadmap?



Universities interested in partnering with DIR to establish RSOCs were asked to provide thorough responses to a series of questions that helped inform DIR of a potential partner's capabilities and resources that could be used for this initiative. Questions included whether the university had an existing security operations center; the people, technologies, and processes that could be used to establish the RSOC stakeholder base; and their overall vision for including university students that may be able to support and or train at the RSOC to provide more qualified and trained workers in the cybersecurity field in Texas. Interested universities were also asked to provide their vision for supporting local governments, school districts, and other entities via the RSOC and leveraging existing community engagement and partners relating to cybersecurity.

In April 2022, DIR notified Angelo State University that it was selected as the pilot RSOC. From July 2022 through December 2022, DIR and Angelo State defined the operating model for the RSOC, establishing core capabilities, and developed student and internship curriculum. The official ribbon cutting ceremony for the Angelo RSOC occurred on January 19, 2023.

In 2023 and 2024, DIR worked with UT and UTRGV to establish both universities as RSOCs. Both universities were part of the original round of submissions during the expression of interest process and were selected for the next round due to their strong proposals. The official ribbon cutting ceremony for the UTRGV RSOC was November 14, 2024. The UT RSOC is currently operationalized and providing service, but it has not had an official ribbon cutting yet.

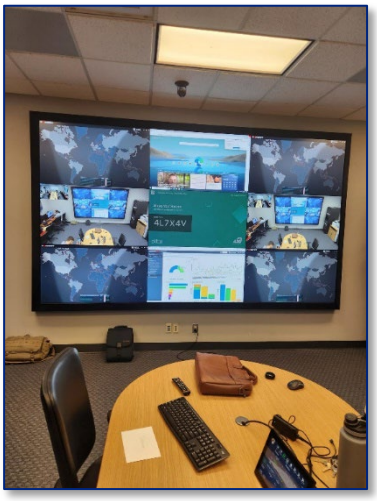
How did you do it?

Collaboration

The sheer size of Texas necessitates collaboration of resources to quickly deploy assistance to entities impacted by a cybersecurity incident.

Technology and Innovation

The RSOCs leverage advanced security technologies and tools for remote incident monitoring, analysis, and response. These technologies can include security information and event management (SIEM) systems, threat intelligence platforms, endpoint detection and response (EDR) tools, and incident management systems. By utilizing these technologies, the RSOCs can efficiently gather, correlate, and analyze security data from multiple sites, facilitating faster response and remediation.



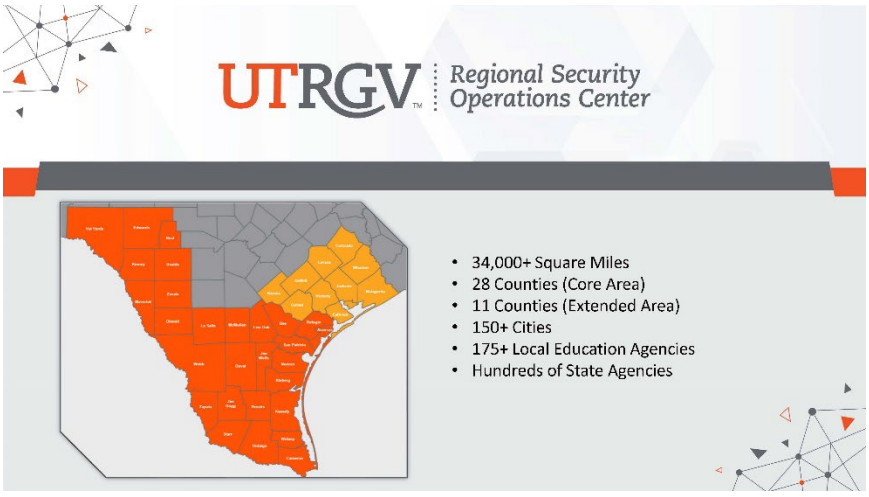
Key features of the RSOC project include endpoint protection, 24x7 threat detection and response, network detection and response (NDR), threat intelligence, and expandable and scalable cybersecurity services to include incident response services.

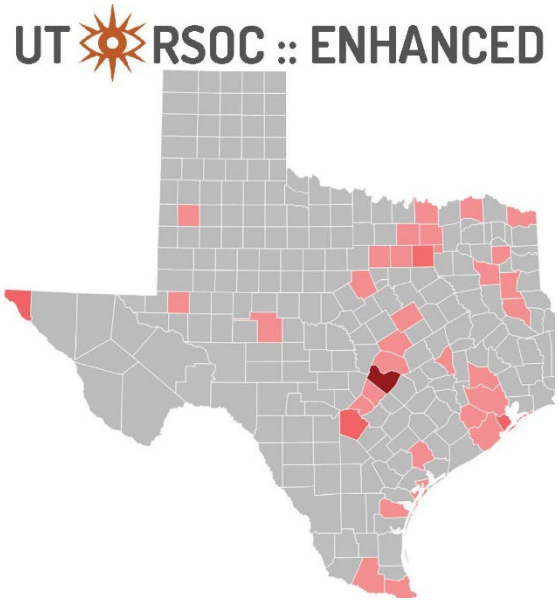
Impact

What did the project make better?

With RSOCs in place, eligible organizations in counties across Texas can optimize the allocation of resources. With geographically dispersed incidents in a state as vast as Texas, it may not always be feasible to have onsite security personnel or experts at every location. This resource optimization allows for efficient incident response and ensures that expertise and knowledge are shared across the organization, benefiting all geographically dispersed locations.

As of May 2025, the ASU RSOC has enlisted 63 student cybersecurity analysts that progress through various tiers of cybersecurity college courses; the UT RSOC has enlisted 31 students, and the UTRGV RSOC has enlisted 23 students. The RSOCs currently serve 65 counties in the West, Central, and Rio Grande Valley areas of Texas.





How do you know?

The objective of the RSOCs is to provide real-time network security monitoring to detect and respond to network security events that may jeopardize participating organizations and the residents of this state. It also

provides alerts and guidance for defeating security threats. In the spirit of IT collaboration, the success of the RSOC relies on the partnerships between DIR and Texas public universities to give university students the training and experience to begin careers in cybersecurity.

"This partnership is not just about providing services that we have but building a coalition across South Texas that will better respond to the needs of securing the citizens of the state. For students, we aim to help them gain the foundational skills they need to walk out with their degree directly into a job and be effective on day one." ***- Dr. Kevin Crouse, DBA, UTRGV Chief Information Security Officer***

"Having the RSOC available at the university creates valuable opportunities for students interested in the field of cybersecurity…It not only opened doors but also allowed me to develop highly valuable skills that have strengthened my foundation in the field." ***-Lizbeth Jaime, UTRGV Analyst Trainee***

What now?

The RSOCs meet the objectives set forth by state leadership through collaboration between the state and public universities. Texas has improved the state's cybersecurity posture by establishing RSOCs in regions across the state. 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 RSOCs in public institutions of education, Texas can concurrently improve the quality and quantity of Texas' cybersecurity analysts by employing and training student analysts in the RSOC.

Additional Project Information and Links

More on the Texas RSOCs can be found at:

Angelo State University: https://www.angelo.edu/community/kay-bailey-hutchison-center/regional-security-operations-center/

Texas Department of Information Resources: https://dir.texas.gov/news/dir-partners-angelo-state-university-pilot-regional-security-operations-center

University of Texas at Austin: https://ut-rsoc.org/

University of Texas Rio Grande Valley: https://rsoc.utrgv.edu

An Overview of Regional Security Operations Centers in Texas (RSOC White Paper): https://dir.texas.gov/sites/default/files/2024-01/An%20Overview%20of%20RSOCs%20in%20Texas%20Jan%202024.pdf