Transforming How Texas Government Serves Texas

Regional Security Operation Center (RSOC) Expression of Interest Overview

Texas Department of Information Resources
December 2021

Table of Contents

The Texas Department of Information Resources (DIR) 1

Background 1

Legislative Reference 2

Introduction to Regional Security Operations Center Pilot Project Proposal 2

RSOC Eligible Services 3

RSOC Eligible Customers 4

Response Information and Instructions 4

Schedule of Events 4

Expressions of Interest 4

Instructions for Submission 5

The Texas Department of Information Resources (DIR)

DIR is responsible for leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.

DIR provides IT products and services to state agencies, institutions of higher education, and other public entities so that those customer organizations have the technological tools to focus on their missions.

DIR's programs provide streamlined technology purchasing for a wide variety of information technology products and services including:

- **Cooperative Contracts**: Hardware, software, staffing services, maintenance, managed services, technology training, DBITS, and other products/services with high customer demand.
- **Shared Technology Services**: Mainframe, server, network, data center, and print/mail services.
- **Information Security**: Products and services to assure the integrity, availability, and confidentiality of information assets.
- **Telecom**: Capitol Complex Telephone System telephone, TEX-AN voice and data services, plus wireless, conferencing, and managed services.
- **Texas.gov**: Payment processing, custom app development, technology and operations, customer service, marketing, and more.

Cybersecurity is one of DIR's core responsibilities. In the event of a major cybersecurity event, DIR is responsible for leading the state's incident response activities as identified in the cybersecurity support function of the State of Texas Emergency Management plan, maintained by the Texas Division of Emergency Management.

For additional information about DIR, please visit: http://dir.texas.gov.

Background

As cyberthreats to public entities continually increase, government entities in all regions need to be protected against attacks that can disrupt the delivery of services or compromise Texan's information.

Since 2019, DIR is aware of at least 115 ransomware events that impacted Texas government organizations — 87 percent of which occurred at the local level. The actual number of ransomware and other cyberattacks against local entities may be even greater because there is no mandatory reporting requirement that local governments report cyberattacks to the state. Still, the sheer number of ransomware events targeting counties, cities, and school districts indicate that cybersecurity programs at the local level needs strengthening. Exhibit 1 reflects the number of ransomware events that DIR is aware of that impacted Texas governments entities since 2019.

Exhibit 1: 2019 through September 2021 Texas Ransomware Events

Organization Type	Number of Incidents
Cities	35
Counties	16
School Districts	39
Other Local Entities	10
State Agencies/Universities	15

In the 2020 Cybersecurity Report, DIR recommended that the legislature create Regional Security Operations Centers (RSOC) located at universities around the state to provide for "boots on the ground" close to local governments that need assistance with major cybersecurity incidents, as well as network security infrastructure that regional governments can utilize.

The RSOC recommendation was included in Senate Bill 475, passed in the 87th Session of the Texas Legislature, and codified in Texas Government Code Chapter 2059, Subchapter E.

In addition to the passage of SB 475, the legislature affirmed its support of this project by appropriating to DIR several full-time employees and general revenue funding to establish the first RSOC with the university partner.

Legislative Reference

The full legislation can be found in Texas Government Code Chapter 2059, Subchapter E – Regional Security Operations Centers.

Introduction to Regional Security Operations Center Pilot Project Proposal

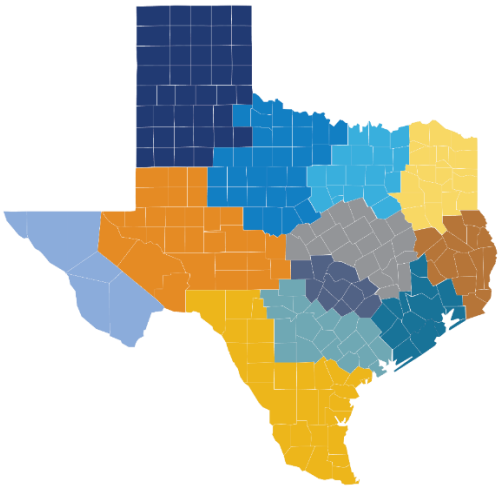
DIR is currently seeking proposals from Texas public universities interested in partnering with DIR to meet SB 475's objectives by operating the pilot RSOC and providing security services and incident response to eligible regional entities.

The university partner selected for the pilot RSOC will play a critical role in the foundation of this program and its future success.

SB 475 allows DIR to establish additional RSOCs if the department determines the first center successfully provides eligible entities the contracted services. DIR envisions eventually expanding to multiple RSOCs located at universities in each of the Comptroller of Public Accounts' twelve economic regions across Texas. Regional security operations centers will provide additional protection across the state and help ensure all governments in Texas can provide continual, secure services to Texans.

The Texas Comptroller's office divides the 268,000 square miles of Texas into 12 economic regions, each with at least one census-defined metropolitan statistical area (MSA) with relatively high population densities and close economic integration (Exhibit 1).

Exhibit 1
Map of Texas Comptroller Economic Regions and Metropolitan Statistical Areas



RSOC Eligible Services

Government Code Section 2059.204 permits DIR and its university partner to offer participating entities the following security services through the RSOCs:

1. **Real-time network security monitoring** to detect and respond to network security events that may jeopardize participating organizations and the residents of this state;
2. **Alerts and guidance** for defeating security threats;
3. **Immediate response** to counter security activity that exposes participating entities and the residents of this state to risk including remote and onsite cybersecurity incident responders;
4. **Policy and Planning** to provide guidance on cybersecurity policies and plans to improve the cybersecurity posture of RSOC customers; and
5. **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.

DIR's vision in partnering with a university to establish the RSOC is to provide students hands-on experience in cybersecurity. While not specially mentioned in the enacting statute, a crucial element of the RSOC is engaging students to participate in providing RSOC services, providing them valuable hands-on work experience while also offsetting staffing costs.

Regional Security Operations Center				
Real-time Security Monitoring	Security Alerts and Guidance	Immediate Response	Policy and Planning	Cyber Education and Awareness
Student Engagement and Workforce Development				

RSOC Eligible Customers

Once the RSOC is established, DIR envisions enlisting, enrolling, and providing cybersecurity services to local, regional, and state entities near the RSOC with the goal of strengthening the region's cybersecurity posture.

Per Government Code Section 2059.201, entities eligible to receive services from the RSOC include:

- Cities
- Counties
- Independent School Districts
- Special Districts
- Independent organization as defined by Section 39.151, Utilities Code
- Public Junior Colleges
- State Agencies

Response Information and Instructions

Schedule of Events

DIR reserves the right to change the dates shown below.

Event	Date
DIR RSOC proposal posted	January 2022
University RSOC EOI Expression of Interest proposal due	No Later Than 31 Feb, 2022
Finalists' interviews and partner selected	April-May 2022

Expressions of Interest

Universities interested in partnering with DIR to establish the pilot RSOC should provide thorough responses to the series of questions below, which are designed to help inform DIR of a potential partner's capabilities and resources that could be used for this initiative.

- Does the university have an existing security operations center that would serve this purpose? If so, how many full-time and part-time employees do you have supporting the SOC? How many endpoints, websites, customers, and/or applications are currently being monitored and serviced by the SOC?
- If the university does not have an existing security operations center, what is the plan, timeline, and proposed location for establishing the RSOC?
- Explain the RSOC road map including the people, technologies, and processes used to establish and to expand RSOC customer base. Include the number of employees and funding required from DIR to support this initiative.
- Explain your vision for including university students that may be able to support and or train at the RSOC in order to provide more qualified and trained workers in the cybersecurity field in Texas.

- Explain your vision for supporting local governments, school districts, and other entities via the RSOC.
- What existing community engagement and/or partners do you have relating to cyber?
- Explain why geographically your university should be selected for the RSOC pilot.
- Specify performance measures that you will track and share to show success of this pilot.
- Provide any additional information explaining why the university should be selected as the RSOC pilot partner. This information may include reports, studies, websites, or other publications from the university.

Instructions for Submission

Universities interested in the RSOC partnership may schedule a meeting to discuss questions or seek clarification by contacting RSOCS@dir.texas.gov.