An Audit of the Regional Security Operations Center at Angelo State University

- The RSOC's projected operating costs exceed its funding due to expansion of operations, and its current levels of spending are not sustainable.
- The RSOC followed its cybersecurity processes, but it could not demonstrate that it appropriately responded to all cybersecurity detections.
- The RSOC did not establish consistent contract terms and conditions with its clients, which could create ambiguity and uncertainty when responding to identified cybersecurity incidents.

Lisa R. Collier, CPA, CFE, CIDA
State Auditor

The Regional Security Operations Center (RSOC) at Angelo State University (University) significantly increased the number of clients receiving its cybersecurity monitoring services without appropriately planning for the accompanying increase in operating expenditures.

The RSOC complied with expenditure and reporting requirements and followed its processes for responding to cybersecurity detections. However, the RSOC did not maintain records of all cybersecurity detections, establish consistent contract terms and conditions, verify that external access to its systems was appropriate, or ensure that all staff completed and maintained required training and certifications.

This audit was conducted in accordance with Texas Government Code, Sections 321.013 and 321.0132.

PRIORITY

FINANCIAL OPERATIONS AND EXPENDITURES

The RSOC significantly increased the number of clients it serves, but it did not ensure that it had sufficient resources to support its existing clients and planned expansion.

Chapter 1 | p. 4

HIGH

CYBERSECURITY MONITORING

The RSOC followed its processes for cybersecurity detection investigations; however, it did not retain all required documentation and establish consistent contract terms and conditions for all clients.

Chapter 2 | p. 9

HIGH

USER ACCESS AND STAFFING

The RSOC maintained appropriate access for internal users, but not for some external users. The RSOC did not ensure that all staff completed or maintained required trainings and certifications.

Chapter 3 | p. 13

For more information about this audit, contact Audit Manager Valerie Bogan or State Auditor Lisa Collier at 512-936-9500.

September 2026 | Report No. **27-001**

Summary of Management's Response

Auditors made recommendations to address the issues identified during this audit, provided at the end of each chapter in this report. The RSOC agreed with the recommendations.

Ratings Definitions

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

PRIORITY: Issues identified present risks or effects that if not addressed could ***critically affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

HIGH: Issues identified present risks or effects that if not addressed could ***substantially affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

MEDIUM: Issues identified present risks or effects that if not addressed could ***moderately affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

LOW: The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks ***or*** effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on the methodology for issue ratings, see Report Ratings in Appendix 1.

Background Information

Regional Security Operations Centers

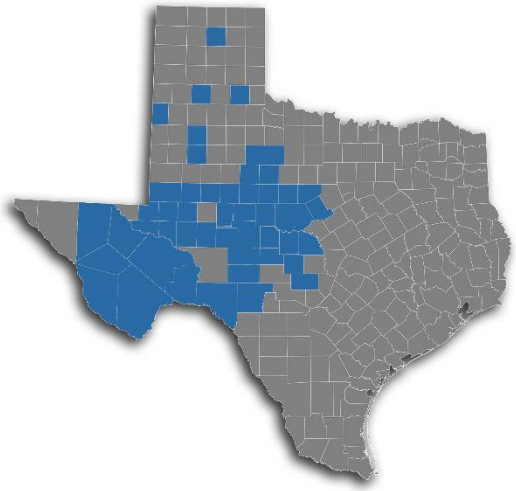
The 87th Legislature passed Senate Bill 475 to implement additional cybersecurity measures throughout the state in response to an increasing number of ransomware and cyberattacks impacting government entities. As a result, the Department of Information Resources (Department) partnered with higher education institutions to establish Regional Security Operations Centers to provide cybersecurity support to local government entities.

The Department established the state's first Regional Security Operations Center in 2022 in partnership with Angelo State University (University). The University Regional Security Operations Center (RSOC) provides real-time network security monitoring, network security threat alerts, incident response, and cybersecurity education to local, regional, and state entities, including counties, municipalities, special districts, school districts, junior college districts, and other political subdivisions of the state.

The RSOC entered into its first interlocal cooperation (ILC) contract with a client in December 2022 and began providing cybersecurity services in March 2023. As of March 2026, the RSOC provided services to 115 entities. Figure 1 shows a map of its clients' locations by county.

Figure 1

RSOC Client Distribution by County as of March 2026



Source: The RSOC.

PRIORITY

Chapter 1
Financial Operations and Expenditures

The Regional Security Operations Center (RSOC) at Angelo State University has rapidly expanded its cybersecurity monitoring operations without appropriately planning for the accompanying increase in operating expenditures.

The RSOC's current levels of spending are not sustainable.

The RSOC started fiscal year 2025 with 37 clients (see text box for information about RSOC clients). That number increased to 68 clients at the end of fiscal year 2025 and then to 115 clients at the end of March 2026 (a 211 percent increase).

As more clients are added, the number of devices requiring monitoring, cybersecurity threats requiring investigating, and staff workload all increase.

The RSOC's largest expenditure is its endpoint detection and response (EDR) monitoring application. The RSOC must purchase a license for each endpoint (see text box for definition) it protects. EDR monitoring costs the RSOC more than $3.5 million per year for the 115 clients it served as of March 2026. Figure 2 on the next page shows the increase in endpoints monitored by the RSOC.

RSOC Clients and Contracts

RSOC clients include local, regional, and state entities (such as city governments and school districts) with whom the RSOC contracts to provide cybersecurity monitoring services. These services are free for all eligible entities because the Department contracts with universities to operate RSOCs using funding from legislative appropriations.

Sources: Texas Government Code, Chapters 2059 and 2063; the RSOC; and the Department.

Endpoints

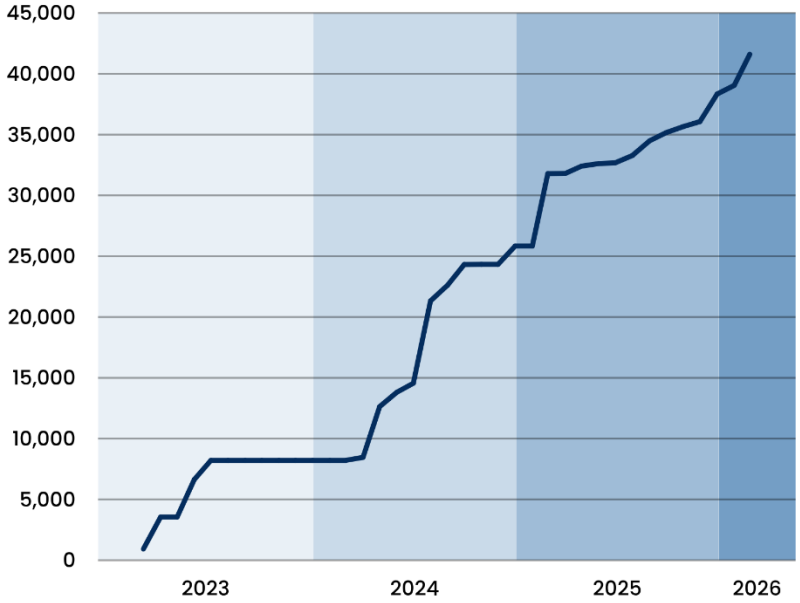
Endpoints are any device that is used to access a network, such as servers and computers. Each client has multiple endpoints.

Because endpoints are a significant target for cyberattacks, it is critical they be monitored.

Sources: National Institute of Standards and Technology and the Cybersecurity & Infrastructure Security Agency.

Figure 2

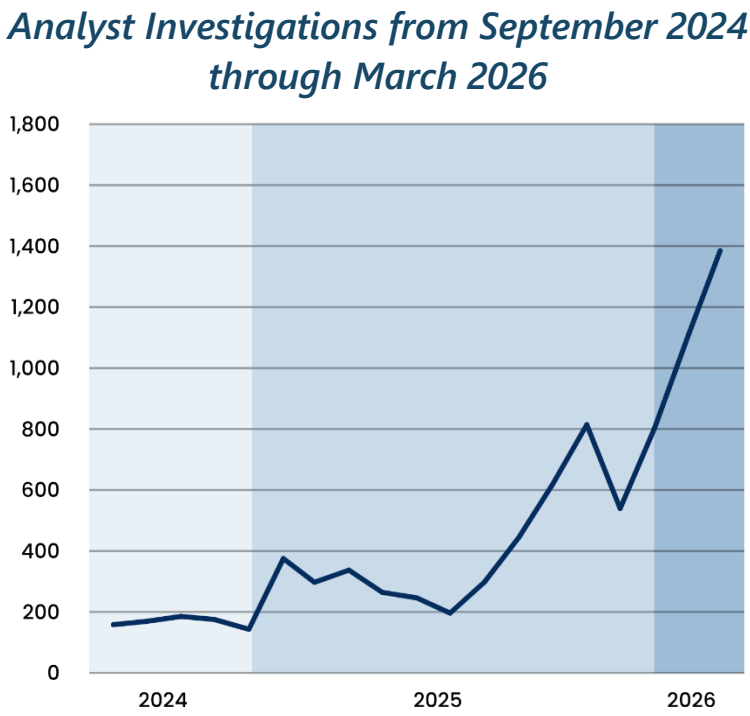
Endpoints Monitored from March 2023 through March 2026



Source: The RSOC.

In addition, RSOC staff was required to investigate and respond to a significantly greater number of cybersecurity threats, an average of 237 per month in fiscal year 2025 compared to an average of 817 per month in fiscal year 2026 as of March 2026 (a 245 percent increase). Figure 3 on the next page shows the increase in analyst investigations conducted.

Figure 3



Source: The RSOC.

The RSOC's sole source of funding is its contract with the Department of Information Resources (Department). In fiscal year 2025, the RSOC's annual operating costs exceeded the $6.1 million it received under its contract with the Department. It sustained its operations using a surplus from prior fiscal years when it served fewer clients.

Without taking on more clients, the RSOC was projected to continue to have budget deficits, requiring it to spend about two-thirds of its remaining surplus funds by the end of fiscal year 2027. However, since March 2026, the RSOC continued to expand and contracted with an additional 72 new clients as of July 2026.

Without securing the operational resources required to provide services to additional clients, the RSOC could extend itself beyond its financial and functional capacity and be unable to meet the increasing demands of adequately monitoring and responding to cybersecurity threats for its clients.

The RSOC's expenditures were allowable, and it provided accurate reports to the Department.

The RSOC had processes in place to ensure that its expenditures were allowable. All 25 of the expenditures tested were allowable, reviewed and approved by the appropriate personnel, and supported by required documentation.

The RSOC also accurately reported to the Department the number of analyst investigations and cybersecurity incidents it closed during calendar year 2025, and the number of clients and endpoints monitored as of March 31, 2026, as required by its Department contract.

Recommendation

The RSOC should regularly assess its costs, financial and staffing resources, and contractual commitments to ensure that its operations are sustainable and it is able to provide adequate levels of cybersecurity monitoring services.

Management's Response

> The RSOC concurs with the recommendation to regularly assess its costs, financial and staffing resources, and contractual commitments to ensure sustainable operations. The RSOC already maintains the financial management practices the recommendation seeks to strengthen. The RSOC conducts monthly Program Management Reviews (PMRs) that review expenditures, staffing, and contractual commitments against funding, and has held regular financial status briefings with both Department of Information Resources (DIR) and Texas Cyber Command (TXCC) leadership to keep leadership informed of resource needs and risks. The RSOC also retains expert consulting support from Martin Jennings of JEC, LLC, who provides independent reviews of financial planning, cost forecasting, and operational sustainability.

To build on these practices, the RSOC will formalize a recurring cost and capacity assessment that ties projected operating costs, staffing levels, and contractual commitments into a single documented review cycle, with results reported, on a scheduled cadence, to university leadership and finally to TXCC leadership for final approval. The RSOC does not operate in an autonomous manner and instead takes its operational and financial direction previously from DIR and currently from TXCC. This enhanced process will be in place by September 30, 2026.

HIGH

Chapter 2
Cybersecurity Monitoring

The RSOC followed its incident response plan when responding to cybersecurity detections; however, its ticket management system did not retain records of deleted cybersecurity threat tickets, increasing the risk that those threats were not addressed. Additionally, some of the RSOC's cybersecurity monitoring contracts lacked provisions to designate responsibilities and support response for cyber threats and attacks.

The RSOC followed its cybersecurity processes, but it could not demonstrate that it appropriately responded to all cybersecurity detections.

The RSOC's ticket management system identified and generated 10,243 cybersecurity threat tickets that the RSOC determined required action between September 1, 2024, and March 31, 2026, for its supported clients. The RSOC classified 26 of those threat tickets as "incidents" because they affected servers or multiple workstations.

- For all 29 threat tickets tested, the RSOC followed its incident response plan and maintained records of notifying client points of contact, analysis, triage activities, resolutions, and closure.
- For all 6 of 26 incidents tested, the RSOC maintained additional records as required, including records showing the timely notification of the RSOC incident commander, detailed incident response reports, executive summaries, and technical details to document the incident response.

However, the RSOC did not consistently maintain records for the threat tickets it determined did not require action because it had deleted some records to reduce the number of tickets in its tracking system. Without those records, the RSOC could not verify that it took appropriate actions for all cybersecurity detections.

In addition, deleting the threat tickets did not comply with the Department's *Security Controls Standards Catalog* and the National Institute of Standards and Technology's *Special Publication 800-53* requirements to track and maintain

records on each incident. After auditors alerted the RSOC about the deleted threat tickets, the RSOC worked with its vendor and as of June 1, 2026, the RSOC's ticket management system was appropriately maintaining copies of all deleted threat tickets.

The RSOC did not ensure contract terms and conditions were consistent for all clients.

The RSOC updated its interlocal cooperation (ILC) contract for new clients in fiscal year 2026 to allow third-party involvement at a client's request (see text box). The RSOC also added several additional provisions to establish protections that were not in previous versions of the RSOC's ILCs, such as:

- Establishing a point of contact (POC) to take immediate action on an RSOC-reported incident or alert and immediately notifying the RSOC of changes to the client POC.
- Exempting the RSOC from liability when the RSOC deploys personnel to assist the client on location and authorizing the RSOC to take action to stop a cybersecurity threat without prior consent of the POC.
- Directing the client to self-report incidents to the Department and acknowledge that the RSOC may share information about incidents with the Department.

Background

In June 2024, an RSOC client experienced a cybersecurity incident that resulted in activating the client's cyber insurance. The insurance company requested access to the RSOC's EDR monitoring application, but the RSOC's contract with the client did not have a clause to grant third-party access to its applications. This delayed and complicated the recovery efforts and prompted the RSOC to update the terms and conditions in its contracts.

Source: The RSOC.

Once executed, the ILCs do not expire unless terminated by one of the parties, and the RSOC did not establish a process to review and update existing ILCs to ensure that the new protections were added to those contracts.

As a result, 27 (79 percent) of 34 ILCs tested did not contain the updated protections.

Without the updates, the ILCs do not sufficiently protect the RSOC from ambiguity and uncertainty regarding appropriate actions to take in response to identified cybersecurity incidents.

Recommendations

The RSOC should:

- Maintain adequate records for all cybersecurity threat detection records.
- Review executed ILC contracts and update outdated contracts as necessary.
- Establish and implement a process to update existing client contracts or execute new contracts or amendments when the RSOC makes changes to ILC language and provisions.

Management's Response

> The RSOC concurs with the recommendations to maintain adequate records of all cybersecurity threat detections, to review and update outdated interlocal cooperation (ILC) contracts, and to establish a repeatable process for updating client contracts when contract language changes. Two points are addressed separately below.
>
> **Maintenance of Cyber Records (Recommendation 2.1).**
>
> The deletion of cybersecurity threat tickets was the result of a technical limitation in the RSOC's ticket management system, which was not retaining copies of deleted records during testing. This was a system behavior, not an intended records practice. The RSOC has already resolved the issue with its vendor, ServiceNow. As of June 1, 2026, the ticket management system appropriately maintains copies of all deleted threat tickets, consistent with the Department's Security Controls Standards Catalog and NIST Special Publication 800-53. In addition, the RSOC engineering team has adopted a documented procedure that prohibits deletion of records during testing and defines how test records are created, used, and disposed of. This control is in place now and will remain in effect.

Refresh of Older ILC Contracts (Recommendation 2.2).

The RSOC acknowledges that older ILCs do not yet contain the updated protections added in fiscal year 2026, including provisions for a designated point of contact, third-party involvement at a client's request, and liability protections. The RSOC is refreshing all older ILCs to the current contract version and forwarding updated contracts to clients for re-execution. Given the number of client contracts involved and the coordination required with each client, this effort will take time to complete. The RSOC has set a target of December 31, 2026, to refresh and re-execute all outstanding ILCs, and will also implement a formal contract review and update process so that future changes to ILC language are consistently applied across all existing and new client contracts.

HIGH

Chapter 3
User Access and Staffing

The RSOC ensured that all internal system users were current employees and had the correct level of user access. However, the RSOC did not ensure that all client points of contact were current and had appropriate access.

Also, the RSOC did not ensure that all staff completed required training and maintained required certifications.

The RSOC maintained appropriate internal user access to its applications but did not ensure appropriate external client access.

The RSOC maintained appropriate access to its information systems for all internal users, but it did not ensure that external client access was appropriate for certain systems. Six of 257 external users of the EDR application and 4 of 433 external users of the ticket management system retained access to those applications up to 5 months after they were no longer the designated contacts.

The RSOC asserted it conducted semiannual periodic user access reviews of external clients; however, it did not document those reviews. In addition, it did not identify the external users who no longer required access to its systems.

The Department's *Security Control Standards Catalog* states that user accounts should be appropriately modified or disabled when users' employment or job responsibilities change. There is a risk that users who retain inappropriate system access could make undetected changes or view sensitive information without the RSOC's knowledge.

The RSOC did not ensure that all staff completed training and maintained certifications as required.

The RSOC established initial and continued training and certification requirements for all staff, which included ethics and cybersecurity awareness training, as well as Criminal Justice Information System (CJIS) certification.

However, of 16 staff tested, 11 were out of compliance with at least one of the trainings or certifications. Specifically:

- Ten staff members did not have current required ethics training. Of these:
  - Seven did not receive initial ethics training when hired and had been employed at the RSOC between 6 and 31 months.
  - Three had not retaken ethics training within two years as required.
- One staff member did not take required cybersecurity awareness training for over 10 months while employed at the RSOC in addition to not fulfilling the ethics training requirement.
- One staff member worked at the RSOC for approximately two months before renewing their lapsed CJIS certification.

The RSOC did not adequately track initial and continued trainings or certifications for its staff. Without required training or certifications, staff may not be aware of appropriate precautions to safeguard the RSOC's sensitive and confidential information.

Recommendations

The RSOC should develop and implement a process to:

- Perform and document periodic reviews of all users and disable access to its systems that is no longer needed.
- Confirm that its staff has met all initial certification and training requirements, and that staff maintains those certifications and training as required.

Management's Response

> The RSOC concurs with the recommendations to perform and document periodic reviews of all users and to confirm that staff meet and maintain required training and certifications. Two points are addressed separately below.

Periodic User Access Reviews (Recommendation 3.1).

The RSOC conducts semiannual periodic user access reviews of internal and external users. The RSOC will conduct quarterly reviews and add formal documentation of each review, including the users reviewed, the access rights confirmed, and any access modified or disabled. This documented process, including timely removal of access for users who no longer require it, will be in place by November 15, 2026.

Staff Training and Certification (Recommendation 3.2).

The RSOC has built a tracking dashboard in ServiceNow that monitors staff completion of required training and certifications tied to Criminal Justice Information System (CJIS) certification. This system is in place now. In coordination with ASU IT and ASU HR, the RSOC will expand the tracking to include initial and recurring ethics (ASU HR) and cybersecurity awareness (ASU IT) training and certification. Tracking metrics will be added to the monthly Program Management Reviews provided to ASU leadership to ensure continued compliance. This enhanced tracking will be fully implemented by September 30, 2026.

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether Angelo State University (University) had processes and related controls to ensure that it operated its Regional Security Operations Center (RSOC) in compliance with applicable requirements and in support of its mission.

Scope

The scope of this audit covered the RSOC's operations from September 1, 2024, through March 31, 2026.

The scope also included a review of significant controls related to the RSOC's operations.

Methodology

We conducted this performance audit from February 2026 through August 2026 in accordance with generally accepted government auditing standards.

The following members of the State Auditor's staff performed the audit:

- Tony White, CFE (Project Manager)
- Matthew Page, CISA (Assistant Project Manager)
- Ethan Clayton
- Andrew Mohr
- Bianca F. Pineda, CIA, CISA, CFE, CGAP (Quality Control Reviewer)
- Valerie Bogan, CIA, CFE (Audit Manager)

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with *Government Auditing Standards* were communicated to University and RSOC management for consideration.

Addressing the Audit Objective

During the audit, we performed the following:

- Interviewed University and RSOC staff to gain an understanding of the RSOC's operations, processes, and related controls.
- Identified the relevant criteria:
  - University, RSOC, and Texas Tech University System policies and procedures.
  - Texas Government Code, Chapters 2059 and 2063.
  - The Department of Information Resources (Department) and the RSOC's interagency cooperation contract.
  - The RSOC and clients' interlocal cooperation (ILC) contracts.
  - The Office of the Comptroller of Public Accounts' *State of Texas Procurement and Contract Management Guide*, versions 3.0 and 4.0.
  - The Department's *Security Control Standards Catalog*, version 2.2.
- Conducted tests of RSOC processes and related controls for compliance with applicable requirements, including:
  - Testing expenditures and procurement card purchases to determine whether financial transactions were allowable, supported, approved, and accurately recorded.
  - Reviewing whether the RSOC followed its incident response plan and maintained documentation of cybersecurity threats and incidents.
  - Testing a sample of RSOC staff to determine whether required employment training and certifications were obtained and maintained.

- Testing user access of the RSOC's critical information technology applications, including its Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) monitoring applications, ticket management system, and administrative management applications.
- Reviewing client contracts to ensure client responsibilities, terms, and conditions were standard in executed client contracts.
- Analyzing the RSOC's operations, including funding, expenditures, clients, cybersecurity threats, and staffing to determine the effects from the expansion of services on its financial and functional capacity.

Sampling Methodology

Auditors selected nonstatistical targeted samples and stratified random samples of:

- Expenditures for software application purchases, consulting, payroll, procurement cards, and travel.
- Critical or high-priority threat tickets generated by the RSOC's EDR and NDR monitoring applications.
- Cybersecurity incidents.
- RSOC staff members.
- Signed interlocal cooperation contracts.

Figure 4 on the next page shows the populations and samples selected for testing.

Figure 4

Populations and Samples Selected

Sampled Items	Population	Sample Size	Sampling Methodology[1]
RSOC Expenditures	412	25	Targeted
NDR Tickets	1,823	7 random, 1 targeted	Stratified Random with Targeted
EDR Tickets	4,664	18 random, 3 targeted	Stratified Random with Targeted
Cybersecurity Incidents	26	6	Targeted
Employee Staffing	73	16	Stratified Random
Client Contracts	163	34	Targeted

Data Reliability and Completeness

To determine data reliability and completeness, auditors:

- Interviewed University and RSOC staff.
- Reviewed data queries and report parameters.
- Observed University and RSOC staff extract data from its systems.
- Analyzed the data to determine whether the information conformed to the auditors' expectations.
- Reviewed user access for key systems.

Based on that work, auditors determined the following data sets were sufficiently reliable for the purposes of the audit:

- Revenue and expenditure data from the RSOC's administrative management system.
- Cybersecurity threat tickets and incidents from the RSOC's ticket management system.
- The population of all former and current RSOC staff.
- Clients that signed an ILC for cybersecurity monitoring services.

[1] Targeted and/or stratified samples are not representative, and it would not be appropriate to project those test results to the populations. Samples were stratified to reflect the makeup of the populations and/or targeted to address specific risk factors in the populations.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dustin Burrows, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

The Regional Security Operations Center at Angelo State University

Members of the Texas Tech University System Board of Regents

Mr. Brandon Creighton, Texas Tech University System Chancellor

Mr. Ronnie D. Hawkins Jr., Angelo State University President