

May 3, 2006

Members of the Legislative Audit Committee:

Security over the Texas lottery is generally satisfactory, but the Texas Lottery Commission (Commission) should correct certain significant security-related weaknesses, particularly in the area of system access. Auditors identified multiple areas in which the Commission should improve monitoring.

To minimize the risks associated with public disclosure, this report summarizes the weaknesses in security identified during this audit, but it does not reveal specific vulnerabilities. Auditors provided the Commission with a confidential report that details the issues identified during this audit. The Commission fully agreed with the recommendations in that report.

Lottery computer, data communications, database, and systems security should be improved.

The Commission does not sufficiently document and enforce policies and procedures to protect its automated resources, including policies and procedures regarding:

- Administrator and special access accounts, including rules for the creation, use, monitoring, control, and removal of accounts with special access privileges.
- Network access, including rules for accessing and using network infrastructure.
- Password and user authentication, including rules for creating, using, distributing, safeguarding, and terminating passwords.
- Intrusion protection, including policies regarding firewalls and intrusion detection systems.

Requirement for this Audit

Texas Government Code, Section 466.020(e), specifies that, at least once every two years, the Commission's executive director must employ an independent firm to conduct a comprehensive study of all aspects of lottery security, including:

- Lottery personnel security
- Sales agent security
- Lottery operator and vendor security
- Security against ticket counterfeiting and alteration and other means of fraudulent winning
- Security of lottery drawings
- Lottery computer, data communications, database, and systems security
- Lottery premises and warehouse security
- Security of distribution of tickets
- Security of validation and payment procedures
- Security involving unclaimed prizes
- Security aspects of each lottery game
- Security against the deliberate placement of winning tickets in lottery games that involve preprinted winning tickets by persons involved in the production, storage, transportation, or distribution of tickets
- Other security aspects of lottery operations.



- Antivirus maintenance, including policies regarding maintaining current antivirus protection.

The Commission also should ensure that it runs the most current versions of its operating systems, implement necessary segregation of duties, strengthen access monitoring, and improve its monitoring of the contracted lottery operator's off-site tape storage.

The Commission should require instant ticket vendors to institute effective disaster recovery controls. It should also ensure that the contracted lottery operator's automated systems are protected from unauthorized access and that it has adequate firewalls, require the lottery operator to improve its disaster recovery controls and implement necessary segregation of duties, and ensure that the lottery operator strengthens its access monitoring.

Lottery operator and vendor security should be improved.

The Commission does not effectively ensure that proper background investigations have been performed for employees of its contracted lottery operator. It also does not monitor and maintain information on a regular basis regarding the status of background investigations performed on employees of the lottery operator. The Commission should also ensure that all lottery operator personnel receive security awareness training.

Security of validation and payment procedures should be improved.

The Commission should implement controls to ensure that it enforces winner eligibility statutes. Currently, the Commission does not have sufficient controls to prevent the award of Texas lottery prizes to statutorily ineligible players. For example, although the spouses of Commission employees are statutorily prohibited from playing or winning lottery games, the Commission lacks controls to prevent or detect the payment of lottery prizes to those individuals. The Commission also should improve its annuity payment tracking process.

Three areas were generally satisfactory but require critical improvements in specific areas:

- Security aspects of each lottery game. The Commission should continue to improve the security associated with the transfer of instant ticket winner data from its ticket manufacturers.
- Security of distribution of instant tickets. The Commission should:
 - ♦ Continue to improve controls over instant ticket returns.
 - ♦ Create controls and procedures for the handling of on-line tickets sent by retailers for credit.
 - ♦ Finalize procedures for its security department's use of tickets for investigations and testing.
 - ♦ Document policies and procedures for the return of instant tickets from couriers.
- Lottery premises and warehouse security. The Commission should consistently enforce its building access policies and procedures and improve the safety of record storage at all claims centers. It should work with its vendors to make necessary security improvements.

Two areas were generally satisfactory but require improvements in specific areas.

- Security of lottery drawings.
- Lottery personnel security.

Auditors did not identify any security issues in four areas.

- Sales agent security.
- Security against ticket counterfeiting and alteration and other means of fraudulent winning.
- Security involving unclaimed prizes.
- Security against the deliberate placement of winning tickets in lottery games that involve preprinted winning tickets by persons involved in the production, storage, transportation, or distribution of tickets.

Resumption of lottery games after a disaster is completely dependent upon the contracted lottery operator, which maintains all systems that run lottery games. The Commission has procedures that enable it to resume the operation of internal administrative systems that support only the Commission's internal accounting system and other internal processes, but it should continue improving those procedures.

It is important to note that the contracted lottery operator (and not the Commission) controls the systems that run all lottery games, including all online games such as Lotto Texas and all instant ticket games. Therefore, the time needed to resume Texas lottery game operations after a disaster is completely dependent on the lottery operator's disaster readiness. To test its back-up site's capability to run lottery games, the contracted lottery operator runs lottery games from its back-up site approximately once a month. Although auditors did not fully test the contracted lottery operator's back-up site, we identified weaknesses in the lottery operator's disaster recovery plan that should be corrected to better ensure that the operation of Texas lottery games can resume promptly after a disaster.

The Commission's recovery center supports only the Commission's internal accounting system and other internal administrative processes. The Commission's current procedures enable it to resume these operations within a reasonable time span after a disaster. The Commission should improve certain aspects of its disaster recovery plan for resumption of operations at that center. For example, it should document critical systems in its disaster recovery plan and identify, perform, and document formal tests of recovery operations.

The reorganization of the Commission's security division has not had a materially adverse effect on security.

The Commission underwent a significant reorganization in November 2004. The reorganization included a reduction in force that could have affected some security functions. Auditors concluded that the reorganization did not have a materially adverse effect on security.

Modifying statute could improve the effectiveness and efficiency of the Commission's security audit.

Statute requires the Commission to obtain an audit covering certain specific areas, regardless of the risk associated with

Summary of Objectives, Scope, and Methodology

The audit objectives were to:

- Meet the statutory requirements of Texas Government Code, Section 466.020, which requires the Commission to obtain a comprehensive study of all aspects of lottery security.
- Investigate concerns regarding the Commission's business resumption/disaster recovery site.
- Determine the effect of the Commission's reorganization on its Security Division.

The audit scope covered January 2005 through November 2005.

The audit methodology consisted of conducting interviews; collecting and reviewing information; and performing tests, procedures, and analyses against predetermined criteria.

This audit was conducted in accordance with generally accepted government auditing standards.

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

- Gregory Scott Adams, CPA, CGFM, MPA (Project Manager)
- Jennifer Wiederhold (Assistant Project Manager)
- Mary Goldwater
- Gary Leach, CQA, MBA, CISA
- Adama Thiam
- Worth Ferguson, CPA (Quality Control Reviewer)
- Ralph McClendon Jr., CISSP, CCP, CISA (Audit Manager)

each area. Requiring a risk-based audit approach would improve the effectiveness and efficiency of the Commission's security audit because it would enable auditors to identify the most high-risk areas and concentrate resources on those areas. Proposed statutory modifications are presented in the attachment to this letter.

We appreciate the cooperation and assistance of Commission staff during this audit. If you have any questions, please contact Ralph McClendon, Audit Manager, or me at (512) 936-9500.

Sincerely,

John Keel, CPA
State Auditor

Attachment

cc: Members of the Texas Lottery Commission
Mr. C. Tom Clowe, Jr., Chair
Mr. James A. Cox, Jr.
Mr. Anthony J. Sadberry, Acting Executive Director, Texas Lottery Commission



This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our Web site: www.sao.state.tx.us.

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.

Attachment

Proposed Statutory Changes to Improve the Efficiency and Effectiveness of the Texas Lottery Commission's Security Audit

Modifying the statutory requirements for the Texas Lottery Commission's security audit would improve the effectiveness and efficiency of the audit. The current statute requires the audit to cover certain specific areas, regardless of the risk associated with each area. Requiring a risk-based audit approach would improve the effectiveness and efficiency of that audit because it would enable auditors to identify the most high-risk areas and concentrate resources on those areas.

Suggested modifications to the current statute are presented below:

Texas Government Code, Section 466.020 (e):

At least once every two years, the executive director shall employ an independent firm that is experienced in security, including computer security and systems security, to conduct ~~a comprehensive study~~ an audit of all aspects of lottery security, including: ~~The scope of the audit shall be determined through a risk assessment performed by the independent auditor.~~ The risk assessment shall consider all aspects of lottery security, including:

- (1) lottery personnel security;
- (2) sales agent security;
- (3) lottery operator and vendor security;
- (4) security against ticket counterfeiting and alteration and other means of fraudulent winning;
- (5) security of lottery drawings;
- (6) lottery computer, data communications, database, and systems security;
- (7) lottery premises and warehouse security;
- (8) security of distribution of tickets;
- (9) security of validation and payment procedures;
- (10) security involving unclaimed prizes;

- (11) security aspects of each lottery game;
- (12) security against the deliberate placement of winning tickets in lottery games that involve preprinted winning tickets by persons involved in the production, storage, transportation, or distribution of tickets; and
- (13) other security aspects of lottery operations.