TEXAS LOTTERY

Texas Lottery Commission
2002 Lottery Security Audit Report
*** Public ***

JEFFERSONWELLS
INTERNATIONAL

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Jefferson Wells International ("Jefferson Wells") recently completed a comprehensive audit and evaluation of security related to the computer systems and business operations for the lottery games of the Texas Lottery Commission ("Texas Lottery") in accordance with the State Lottery Act. The engagement was performed between October 7, 2002, and December 6, 2002.

Request For Proposals ("RFP") 362-2-1291 issued by the Texas Lottery on June 6, 2002 defined the requirements for the audit. Audit work was performed at the Texas Lottery; the Texas Lottery's operator, GTECH Texas; and the Texas Lottery's instant ticket manufacturer, Scientific Games International.

Engagement Objectives and Approach

The audit's overall objective was to perform an assessment of the security established by management to support the integrity, security, honesty, and fairness of the Texas Lottery's operations, gaming services, and instant and on-line ticket productions. In addition, we assessed the computerized gaming system operated by GTECH Texas, as well as the general and application controls for Scientific Games International's computerized systems.

To accomplish these objectives Jefferson Wells personnel:

- Met with Texas Lottery management to gain an understanding of the critical Texas Lottery processes;
- Interviewed key Texas Lottery and vendor personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Identified high-risk areas based on impact and likelihood of a control breakdown or a non-existent control;
- Verified the existence and effectiveness of the controls and processes in place to meet the objectives delineated above; and
- Identified vulnerabilities associated with any weaknesses in the control environment.

Our approach was not designed to specifically detect illegalities, fraudulent acts, errors or other irregularities. Our procedures were designed to test high-risk areas based on the scope of the RFP and may not detect every security weakness. Jefferson Wells did not attempt to corrupt or tamper with any Texas Lottery information.

During the course of our audit, we did not identify any issues that would materially impact the fairness or integrity of the Texas Lottery's games. This report documents the issues and risks identified the recommended corrective actions, and the responses from the Texas Lottery and its vendors. Our report is organized as defined in the RFP's section 6.3.4.

* * *

Jefferson Wells is not a public accounting firm and does not provide attest services or otherwise report on financial statements.

6.3.4.1 Follow-up on Previous Security Audit Report Findings

Jefferson Wells performed follow-up audit procedures on previous Security Audit Report findings (report dated 2000 and follow-up to that report dated 2001) in conjunction with performing this year's audit. We determined the current status of follow-up items by interviewing appropriate personnel, reviewing documentation, and observing key controls. Results of our follow-up review are documented in the appropriate sections of this report.

6.3.4.2 Follow-up on SAS #70 Service Audit Report Findings

Jefferson Wells performed follow-up audit procedures on the 2001 GTECH Texas Operations SAS #70 Service Audit Report findings in conjunction with performing this year's audit. We determined the current status of specific issues by interviewing appropriate personnel, reviewing documentation, and observing key controls. Results of our follow-up review are documented in the appropriate sections of this report.

6.3.4.3 Overall Computer Environment Security – Texas Lottery Commission

We performed a detailed technical audit to assess the risks and evaluate the control procedures over physical, logical, and data security that apply to the gaming computer operations, and data/voice telecommunication interfaces between the Texas Lottery, Texas Lottery operator, instant ticket vendors, and retailers. The areas reviewed include Overall Computer Security, Database Security, Systems Security, and Data Communications Security.

Issues, risks, and recommendations from our evaluation are summarized below.

6.3.4.3.a Computer Security - Texas Lottery

Issue # 1 - Information Security Officer

No single individual is specifically responsible for information security and whose primary job function is to "… develop and recommend policies and establish procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction, or disclosure."[1]

Risk #1

The function of information security is spread among numerous individuals in Information Technology ("IT") and is not anyone's primary responsibility. This situation causes a disjointed effort in establishing overall information security as well as significantly differing standards regarding the implementation of specific information security areas. Also, this situation precludes an independent presence that oversees the tactical implementation of information security measures. For example, the Texas Lottery cannot expect Systems Administrators who may have (mistakenly) allowed weak security standards to report that situation of their own volition. 1 TAC §202(d) requires each agency to designate an individual to administer the information security program in that agency.

[1] 1 TAC §202.3(d)(1)

Recommendation #1

The Texas Lottery should designate an individual to administer the information security program for the agency. This individual could be within either the IT or Security department and should be responsible for establishing the information resources security program at the Texas Lottery Commission. Duties, as described in 1 TAC §202(d), should include the following:

> (1) It shall be the duty and responsibility of the Information Security Officer to develop and recommend policies and establish procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information resource assets against unauthorized or accidental modification, destruction, or disclosure.
>
> (2) The Information Security Officer shall document and maintain an up-to-date information security program. The Texas Lottery Executive Director must approve the information security program.
>
> (3) The Information Security Officer is responsible for monitoring the effectiveness of defined controls for mission critical information.
>
> (4) The Information Security Officer shall report, at least annually, to the agency Executive Director the status and effectiveness of information resources security controls.

Texas Lottery Response #1

The agency concurs. An action plan is being developed to identify the appropriate individual for this position.

Issue #2 – IT Security Manual

The primary information security document, the *Information Resources Security Manual*, is out-of-date and needs to be updated.

Risk #2

The lack of a current security document leads to inconsistencies in implementing electronic security features and inefficiencies in security management. Additionally, the lack of a current security manual may manifest itself in inconsistent practices.

Recommendation #2

The Texas Lottery should update the *Information Resources Security Manual* to reflect the current environment and those practices necessary for successful and secure Texas Lottery operations.

Texas Lottery Response #2

The agency concurs. A revision is currently in draft form and is being reviewed. The maintenance of this document will be the responsibility of the Information Security Officer.

Issue #3 –Change Control

Current IT management is not satisfied with change control procedures that have been established at the Texas Lottery and is implementing change control procedures that will create a more controlled environment and provide a better audit trail. These new procedures are currently being drafted. The following change control issues currently exist:

- Programmers, both contract and internal, have the ability to move the programs for which they are responsible into production.
- Version control software is not consistently used to control how programs are moved into production, to log when programs are moved into production and who moved them, and to provide better version control to document what was changed.
- Review of the multiple change control procedures revealed the procedures are incomplete, redundancy exists between the procedures, and the procedures are out of date.
- IT management does not regularly or methodically reviews code changes moved into production.

Risk #3

Change control is the process of managing all significant changes to the Texas Lottery systems environment in a methodical and structured manner so that only authorized changes are made and those changes do not impact the integrity of production operations. Lack of adequate change control can result in unstable systems and possible unauthorized changes to production programs and data.

Recommendation #3

The Texas Lottery should continue their efforts to formalize their change control procedures. Specifically, the Texas Lottery should update current change control procedures to require using version control software (under the control of the Texas Lottery) to control and track all changes to production systems. Procedures should document approval and testing requirements required before a program is moved into production. Programmers should be formally prevented from moving the programs for which they are responsible into production.

Texas Lottery Response #3

The agency concurs. New configuration management tools have been acquired and new procedures are being developed to address this process.

Issue #4 - Business Resumption Planning

The Texas Lottery recently implemented a Storage Area Network (“SAN”) that will provide real time data backup while reducing the risk of human error and the time required to get the alternate site into an operational status. In addition, the Business Resumption Coordinator plays an active role to ensure the plan is complete and up-to-date. The Business Resumption Plan (“BRP”) appears to meet industry “Best Practice Standards”.

The following issues were identified with the Business Resumption Plan:

- The structure of the plan is confusing with few clearly indicated checklists. Several of the checklists in the document are related to emergency actions and therefore people will not likely have the time to read and become familiar with their actions. Page numbering is inconsistent from beginning to end. It is not clear the time frames mentioned in the plan are business time.
- The planned backup communications system is the use of commercial cellular telephones. However, in the event of a widespread outage of the standard commercial telephone system, commercial cellular telephones may not be usable.
- There appears to be some inconsistency regarding the minimum recovery time allocated for critical functions. The IT portion of the plan calls for a four-hour restoration while the master plan calls for an eight-hour restoration period. This is caused by differing priorities within the functions labeled "Critical".
- The plan referenced Rule 1 TAC §201.13 (b) *Information Security Standards*. However, that document has been superceded by 1 TAC §202.6 *Information Security Standards*, dated June 18, 2002.
- The plan should mandate periodic (annual) tests that demonstrate the capability of key personnel to perform their business resumption duties. A requirement for semi-annual fire drills is stated, but not a requirement to test the business resumption functions.
- The existing manner in which backup tapes are rotated off-site to the alternate command center is lacking.

Risk # 4

Without an effective Business Resumption Plan, the Texas Lottery may not be able to recover computer applications required to perform core agency functions, in a timely manner, in the event of a disaster.

Recommendation # 4

Although the Business Resumption Plan appears to be effective, the Texas Lottery Commission should take steps to enhance their Business Continuity Planning efforts by addressing the identified issues.

Texas Lottery Response #4

The agency concurs.

6.3.4.3.b Database Security - Texas Lottery

Issue #5 - Database Security

Jefferson Wells reviewed the Oracle database and the recently implemented Microsoft SQL server database using an automated vulnerability assessment tool and by evaluating database configuration parameters. The following database security weaknesses were noted:

- Database logging is lacking,
- Passwords controls are inconsistent, and
- Various configuration vulnerabilities were identified.

Risk #5

Weaknesses in database logging result in the lack of an audit trail, which increases the risk that, an attacker's actions will not be detected. Inconsistent password controls increase the risk that an attacker can gain unauthorized access to the database.

Recommendation #5

The Texas Lottery should take measures to further strengthen database security. The above database security issues should be addressed.

Texas Lottery Response #5

The agency concurs. Necessary actions will be taken to strengthen database security.

6.3.4.3.c Systems Security - Texas Lottery

Administrative controls to augment the software controls in computer, data communication and database security are addressed in the appropriate sections of the report.

6.3.4.3.d Data Communications Security - Texas Lottery

Issue #6 – Network Security

Jefferson Wells identified a number of issues that impact the security of the Texas Lottery's internal network. These issues include:

- Perimeter security controls,
- Router configurations, and
- Network monitoring.

Risk #6

Perimeter security controls are necessary to prevent attackers from gaining unauthorized access to the Texas Lottery network. While router configurations can be used to filter out unwanted network traffic, network monitoring is required to detect successful and unsuccessful network security attacks.

Recommendation # 6

The Texas Lottery should take steps necessary to address the identified network security issues.

Texas Lottery Response #6

The agency concurs.

Issue #7 Phone Switch and Voice Network

Evaluation of the Private Branch Exchange ("PBX") telephone system identified the following weaknesses:

- Texas Lottery employees are not required to use any kind of pass-code in order to make long distance phone calls,
- Departmental management is not required to review phone bill details of long distance phone calls made from their area(s) of responsibility,
- New phone system user's voicemail accounts *always* have the same default pass-code setup for that new employees first usage,
- Users are never required to change their voicemail pass-code after the initial setup,
- Rotation of nightly backup tapes to the off-site storage facility is not performed on a timely basis,
- The Business Resumption Plan detail regarding PBX restoration is incomplete and inadequate, and
- PBX change control procedures are lacking.

Risk # 7

The above issues could result in improper use of the telephone system and the inability to recover the telephone system in a timely manner in the event of an outage.

Recommendation # 7

The Texas Lottery should take measures to strengthen the PBX system controls.

Texas Lottery Response #7

The agency concurs. The agency will review both PBX and network security.

6.3.4.4 General Controls and Security Review - Texas Lottery

ACCESS

Issue #8 – Windows Servers

Overall, there are several issues regarding the way Windows servers are configured with respect to security. There are missing or vague guidelines for System Administrators to follow. As a result, some inconsistent and/or weak security practices have occurred. Findings were identified in the following areas:

- Password security,
- Remote access,
- Event auditing, and
- File directory permissions.

Risk #8

Windows server configuration issues identified could result in unauthorized disclosure, modification, or deletion of critical Texas Lottery information.

Recommendation #8

The Texas Lottery should take steps necessary to address the identified Windows server configuration issues.

Texas Lottery Response #8

The agency concurs.

Issue # 9 - NetWare Servers

The NetWare network resides on robust hardware and is backed-up by a Storage Area Network to the Texas Lottery Warehouse (also used as the Alternate Command Site). The Texas Lottery cycles passwords every 30 days. This is significantly more rapid than most organizations.

Issues were identified related to account and password weaknesses on the NetWare servers.

Risk # 9

Weaknesses associated with accounts and passwords increase the risk that the NetWare servers could be compromised resulting, in unauthorized disclosure, modification, or deletion of data.

Recommendation # 9

The Texas Lottery should take steps necessary to address the identified NetWare server configuration issues.

Texas Lottery Response #9

The agency concurs. All associated findings have been corrected.

Issue #10 - OpenVMS

The OpenVMS system at the Texas Lottery included a number of controls including robust logging, break-in detection, and timely deactivation of accounts not used within 30 days. Jefferson Wells identified the following issues that may impact the security and administration of the Texas Lottery's OpenVMS System:

- The use of a shared account with powerful system rights,
- Users with access to sensitive system privileges in excess of their business need,
- The need for better documentation of user administration procedures, and
- Various system security setting concerns.

Risk # 10

Because several users and batch jobs use this privileged account, there is no individual accountability. In addition, the risk that the password to this account is compromised is increased because the password is not changed on a regular basis. Inappropriate system settings increase the risk of unauthorized access to the system.

Recommendation # 10

The Texas Lottery should:

- Discontinue the use of shared accounts. If individuals need specific access, it should be granted to the individual's account to maintain an effective audit trail.
- Limit access to sensitive system privileges.
- Update the user and group administration policy to include account maintenance procedures, prohibition of the use of shared accounts, and a requirement for periodic management review of individuals' system capabilities.

Texas Lottery Response #10

The agency concurs.

Issue #11 - ProSys Application

The following issues were noted:

- Currently there is no concise description of the user access profile. The Texas Lottery should develop such a description so Division Directors have a clear understanding of the profile capabilities.
- Division Directors do not receive reports periodically showing PROSYS users within their department and their access capabilities.
- The Executive Director is assigned the SuperUser privilege within ProSys, which provides unlimited access to the ProSys system. If this account were compromised, the attacker would gain unlimited access to ProSys.
- The *ProSys System Administration Functions: Group Profiles Procedure (IT-SA-PR-006)* documents the procedures for adding new users to the system. The procedure does not clearly cover the process for disabling terminated users on the system.

Risk #11

The issues identified above could result in users with unnecessary access to the ProSys application that could result in inappropriate data disclosure, modification, or deletion.

Recommendation #11

The Texas Lottery should take steps to strengthen user administration procedures on the ProSys application. Specifically:

- A description should be created for each of the profiles explaining the access capabilities of the profile.
- Reports showing users and associated ProSys profiles should be produced annually and provided to division management to verify all user access is appropriate.
- Any employee without a need for the Super User capability should have this privilege removed.
- The ProSys System Administration Functions: Group Profiles Procedure (IT-SA-PR-006) should be updated to include procedures for modifying user access, resetting passwords and terminating user access.

Texas Lottery Response #11

The agency concurs. Systems Administration is currently reviewing all user administration procedures.

6.3.4.5.a Texas Lottery and Texas Lottery Operator Personnel Security

Issue #12 – Texas Lottery Personnel Policies and Procedures

During our review of Texas Lottery Personnel Policies and Procedures, we identified the following:

- There is no requirement that personnel policy and procedures be reviewed and updated at least annually.
- Personnel procedures and their associated forms and attachments could be more organized on the "P" drive.
- Although some parts of the Human Resource Personnel Policy Handbook have been revised, other revisions should be considered.
- Some of the acknowledgement forms regarding personnel policies and procedures may require additional explanation.
- With the exception of contract language relating to ethical standards for vendors and vendor employees, there is no comprehensive contract language addressing certain vendor employee standards of conduct.

Risk #12

If forms are out of date, difficult to locate, or not understood their effectiveness is limited. As a result, the risk increases that employees will not be aware of the current personnel policies and procedures. For contractors, risk increases if the vendors and their employees are not aware of certain standards of conduct.

Recommendation #12

The Texas Lottery should enhance their personnel policies and procedures. This could be achieved by:

- Using a more unified method of creating and maintaining personnel policies and procedures, perhaps through an Intranet site that allows a single access location and that incorporates a search engine.
- Requiring annual training of employees regarding IT security responsibilities.
- Using policy-related software to develop online training of ethics, security, and other policies and procedures. Allowing the employees to receive the training at their own workstations at a time convenient to them, thereby, eliminating the need to hold classes.
- Periodically reviewing and revising the *New Hire Orientation Instructor Syllabus* and the *Employee Checklist* to help ensure important items are not overlooked during orientation.
- Developing a handout to cover building security issues. We have forwarded a sample of those currently used by the Texas Lottery claim centers that is very useful. It includes bomb threats and could easily be modified to include chemical spills.
- Including contract language that communicates certain standards of conduct to vendors.

Texas Lottery Response #12

The agency concurs.

6.3.4.5.b Physical Security

Issue #13 – Physical Security

Jefferson Wells reviewed physical security at the Texas Lottery headquarters, primary and backup data centers, and warehouses. We identified several issues including:

- Perimeter security,
- Electrical power,
- Data Center access,
- Data Center fire suppression, and
- Data Center environmental controls.

Risk #13

Physical security risks increase opportunities for valuable assets, including computer assets, to be damaged, stolen, or accessed. Without comprehensive environmental controls in the data center, the risk of loss or damage to vital computer systems and expensive hardware components may increase.

Recommendation #13

The Texas Lottery should take actions to address the physical security issues identified at the agency headquarters, primary and backup data centers, and warehouses.

Response #13

The agency concurs.

6.3.4.5.c Sales Agent Security

NO FINDINGS

6.3.4.5.d Ticket Distribution

NO FINDINGS

6.3.4.5.e Ticket Security

NO FINDINGS

6.3.4.5.f Security of ticket validation and winner payment procedures

Issue #14 – Ticket validation and winner payment procedures

The following issues related to ticket validation and winner payment procedures were identified:

- Incoming Claim Center mail is processed outside of cameras view in a separate work area. File boxes block one of the two cameras and the other camera is unable to capture work activities because the staff sits with their back to the camera.
- Video camera(s) do not include the fireproof safe area at the Austin Claim Center. These file drawers are left open during the day and are subject to support service personnel attending to heating and cooling issues. In addition, if a break-in should occur, this area would not be protected. Sensitive material is kept in these file drawers (check stock, unclaimed prizes and winner information).

Risk #14

These weaknesses could result in inefficient processing of Claim Center mail, inadequate monitoring of mail processing, and insufficient monitoring of the Austin Claim Center safe.

Recommendation #14

The Texas Lottery should enhance their security of ticket validation and winner payment procedures. This could be achieved by the following:

- Improve camera visibility for Claim Center mail processing.
- Policy *SE-PR-050 "Mailroom Investigation"* Step 3.4 should be reviewed for accuracy. We were informed that the number of pieces of mail contained in the mailbag is not recorded at any point.
- Video camera monitoring should include the fireproof safe area at the Austin Claim Center.

Response #14

The agency concurs.

Issue #15 - Texas Lottery Commission Claim Centers Physical and Access Security

Security evaluations of Texas Lottery Claim Centers were performed at six locations that included both large cities (Dallas, Houston, San Antonio) and smaller cities (Austin, Fort Worth, Tyler). The risks observed were, for the most part, consistent and can therefore likely be extrapolated to include Texas Lottery Claim Centers throughout the State of Texas. Jefferson Wells identified a number of issues around physical security at the Claims Center including:

- Lack of video monitoring certain critical areas,
- Claim Center security configurations, and
- Network equipment was sitting unprotected in the back room.

Risk #15

Inadequate physical access and security measures increase opportunities for Texas Lottery employees to be harmed or valuable Texas Lottery assets to be damaged, stolen, or improperly accessed.

Recommendation #15

The Texas Lottery should take measures to address the identified Claim Center Physical Security issues.

Response #15

The agency concurs.

6.3.4.5.g Security involving Texas Lottery unclaimed prizes

NO FINDINGS

6.3.4.5.h Security of Texas Lottery drawings

Issue #16 – Security of Texas Lottery drawings

The Texas Lottery recently decided to discontinue using Texas Lottery Commission Investigators to provide a security presence at the nightly draws.

Risk #16

The security provided by the current contracted security guards is not as effective as the security provided by Texas Lottery Investigators. As a result, the risk increases that the drawings are disrupted.

Recommendation #16

The Texas Lottery should determine the best way to provide security for the nightly drawing by considering the effectiveness of the various security providers (Texas Lottery Investigators, contracted unarmed security, or contracted armed security) and the associated costs as compared to the risk.

Response #16

The agency concurs.

6.3.4.6. Security aspects of each type of Texas Lottery game

Issue #17 – Security Aspects of each type of Texas Lottery game

In reviewing sales agent security we determined procedure SE-PR-001 (9) is not accurate because it has not been updated to incorporate the most recent changes to game audits. In addition, items listed in the Table of Contents do not easily tie to the required items listed in the procedure making it difficult to locate and determine if the proper items have been included. The results of testing found that each of the books we examined was missing at least one of the described required items.

Risk #17

These weaknesses could result in inconsistent game testing and testing documentation, which could result in critical testing procedures not being performed.

Recommendation #17

The Texas Lottery should update/revise procedure SE-PR-001 (9) Ticket Production to clearly and accurately reflect the required items for each Game Book. It would also be helpful to add start and stop dates to change items in this list and keeping discontinued items in the list with their corresponding end date. This additional information will be helpful when evaluating the contents of the books. Where possible, the Texas Lottery should locate and document the identified missing information.

Response #17

The agency concurs.

6.3.4.8 Web-site hosting service

Jefferson Wells did not perform a detailed review at Future Protocol, Inc. since the Texas Lottery is in the process of finalizing an award to another vendor to provide web-site hosting services.

GTECH

6.3.4.3 Overall Computer Environment Security

6.3.4.3.a - Computer Security

No issues identified.

6.3.4.3.b - Database Security

Issue #1 - Database Security

Review of the Sybase database server at GTECH identified the following issues:

- Guest IDs are still on the MASTER database.
- Auditing is not performed on the Sybase database due to performance impact.
- The Sybase databases running on the OLTP systems contain only generic accounts that are shared by multiple individuals. Passwords for these accounts are not changed on a regular basis.

Risk #1

Weaknesses with database security could result in unauthorized access, modification, or deletion of data. The use of shared accounts makes it difficult to tie an action to a specific individual, which results in a lack of accountability.

Recommendation #1

GTECH should take steps to correct these issues by removing the guest account, enabling an appropriate level of logging, and using individual user accounts instead of shared accounts.

Response #1

Will investigate for compliance of Audit suggestions.

6.3.4.3.c – Systems Security

No issues identified

6.3.4.3.d – Data Communications Security

No issues identified

6.3.4.4 General Controls and Security Review

ACCESS

Issue #2 - OpenVMS Issues

Jefferson Wells reviewed the OpenVMS system and identified the following issues:

- Users with excess system privileges,
- Powerful shared accounts are used,
- Inappropriate security configuration settings, and
- Log review processes.

Risk #2

Risk increases that information is inappropriately disclosed, modified, or deleted because of these issues. The use of shared accounts makes it difficult to tie an action to a specific individual, which results in a lack of accountability.

Recommendation #2

GTECH should take measures to increase OpenVMS security. Specifically, the use of system privileges should be limited, shared accounts should never be used, and security settings should be set to industry best practice standards.

Response #2

Will investigate for compliance of Audit suggestions.

Issue #3 - UNIX Server Issues

Issues for the Unix were identified in the following areas:

- System configuration settings,
- Unnecessary services running,
- Excessive user permissions, and
- Inappropriate file permissions.

Risk #3

The Unix issues identified could result in unauthorized disclosure, modification, or deletion of critical information.

Recommendation #3

GTECH should take measures to increase Unix security. Specifically, the unnecessary services should be removed, file permissions should be restricted, and user permissions and security settings should be modified to provide better control.

Response #3

Will investigate for compliance of Audit suggestions.

Issue #4 - Windows Server Issues

Issues for the Windows servers were identified in the following areas:

- Numerous accounts are expired, disabled, or have never logged in before,
- Remote management of the network, and
- Although not domain controllers, other servers have nonstandard password policies.

Risk #4

The accounts that have never logged on can pose a risk in that they can be accessed by anyone who knows the default password. The above issues increase the risk Windows servers could be compromised.

Recommendation #4

GTECH should take measures to increase Windows security. Specifically, GTECH should verify remote management software is used in a secure manner. In addition, the account and password management security settings should be modified to provide better control.

Response #4

Will investigate for compliance of Audit suggestions.

Issue # 5 - ProSys Application

Issues for the ProSys application were identified in the following areas:

- Incomplete documentation of administration procedures,
- Inadequate logging utility ,
- System parameters are not set to IT best practices, and
- ProSys login information is not encrypted.

Risk #5

The issues identified could result in unauthorized access and the inability to detect unauthorized access.

Recommendation #5

GTECH should take steps to address the ProSys application weaknesses identified.

Response #5

Will investigate for compliance of Audit suggestions.

PHYSICAL SECURITY

Issue #6 - GTECH Security Supervisor Administrative/Monitoring Procedures

The administrative and monitoring procedures of the (GTECH) Security Supervisor are not documented.

Risk #6

There may be a lack of continuity of operations in the event of personnel transition.

Recommendation #6

Administrative and monitoring procedures of the (GTECH) Security Supervisor should be formally documented.

Response #6

Will investigate for compliance of Audit suggestions.

Issue #7 – Primary Data Center

Issues for the GTECH Primary Data Center were identified in the following areas:

- Facility entrances,
- Data Center visibility,
- Data Center environmental controls, and
- Data Center organization.

Risk #7

Inadequate physical access security increases opportunities for valuable computer assets to be stolen, accessed, or damaged. There is risk of damage to vital computer equipment and systems, as well as injury to employees.

Recommendation #7

GTECH should take steps to address the weaknesses identified related to the physical security of the Primary Data Center.

Response #7

Will investigate for compliance of Audit suggestions.

Issue #8 - Backup Data Center

Issues for the GTECH Backup Data Center were identified in the following areas:

- Facility entrances,
- Data Center visibility,
- Data Center environmental controls,
- Data Center organization, and
- Facility surveillance.

Risk #8

Inadequate physical access security increases opportunities for valuable computer assets to be stolen, accessed, or damaged. The above issues could result in increased risk of damage to vital computer equipment and systems.

Recommendation #8

GTECH should take steps to address the weaknesses identified related to the physical security of the Backup Data Center.

Response #8

Will investigate for compliance of Audit suggestions.

6.3.4.5 Texas Lottery and Texas Lottery Operator Personnel Security

NO FINDINGS

SCIENTIFIC GAMES INTERNATIONAL

6.3.4.4 General Controls and Security Review

Issue #1 – General Controls and Security

The review of logical security at Scientific Games identified the following issues:

- User-id and password security,
- Other logical security controls,
- Physical security,
- Backup and rotation, and
- Disaster Recovery Plan testing.

Risk #1

Although no high-risk findings were identified, the identified security issues could increase the risk of unauthorized access to operating systems, applications, and files. Physical and environmental security risks increase the opportunities for valuable computer assets to be damaged, stolen, or accessed. Disaster Recovery issues increases the risk that extended computer outages will occur in the event of a disaster.

Recommendation # 1

Scientific Games should take steps to strengthen General Controls and Security by addressing the issues identified.

Response # 1

Scientific Games agrees that no high risk issues were identified.

We do not agree that those low-risk logical security issues that were identified would lead to unauthorized access of operating systems, applications or files. We also do not agree that the identified physical security risks would result in damaged computer assets, stolen computer assets or illicit access of computer assets. Finally, we do not agree that any extended computer outages would occur in the event of a disaster.

Scientific Games will continue to use the latest technology and best-practice policies to ensure that our printing facility in Alpharetta is viable and secure.