



PERFORMANCE AUDIT REPORT

Security in the Operation of the Kansas Lottery

A Report to the Legislative Post Audit Committee

By Delehanty Consulting LLC

**An audit firm under contract with the
Legislative Division of Post Audit**

State of Kansas

December 2007

Legislative Post Audit Committee

Legislative Division of Post Audit

THE LEGISLATIVE POST Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about \$10 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of governmental agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U.S. Government Accountability Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. The standards also have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the Representatives, three are appointed by the Speaker of the House and two are appointed by the Minority Leader.

Audits are performed at the direction of the Legislative Post Audit Committee. Legislators

or committees should make their requests for performance audits through the Chairman or any other member of the Committee. Copies of all completed performance audits are available from the Division's office.

LEGISLATIVE POST AUDIT COMMITTEE

Representative Peggy Mast, Chair
Representative Tom Burroughs
Representative John Grange
Representative Virgil Peck Jr.
Representative Tom Sawyer

Senator Nick Jordan, Vice Chair
Senator Les Donovan
Senator Anthony Hensley
Senator Derek Schmidt
Senator Chris Steineger

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
E-mail: LPA@lpa.state.ks.us
Website:
<http://kslegislature.org/postaudit>
Barbara J. Hinton, Legislative Post Auditor

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.



LEGISLATURE OF KANSAS

LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
E-MAIL: lpa@lpa.state.ks.us

December 10, 2007

To: Members, Legislative Post Audit Committee

Representative Peggy Mast, Chair	Senator Nick Jordan, Vice-Chair
Representative Tom Burroughs	Senator Les Donovan
Representative John Grange	Senator Anthony Hensley
Representative Virgil Peck	Senator Derek Schmidt
Representative Tom Sawyer	Senator Chris Steineger

This report contains general findings and conclusions from the completed performance audit, *Security in the Operation of the Kansas Lottery*. The audit was done by Delehanty Consulting, a firm under contract with the Legislative Division of Post Audit. As provided for under the Kansas Open Records Act, the audit also resulted in a confidential report that gives detailed findings and recommendations regarding security matters.

We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

A handwritten signature in black ink, reading "Barbara J. Hinton". The signature is written in a cursive, flowing style with a large, prominent initial "B".

Barbara J. Hinton
Legislative Post Auditor

EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

Security in the Operation of the Kansas Lottery

The audit addresses all aspects of security in the operation of the Kansas Lottery. Specific areas covered include the following:

- *Personnel security*
- *Retailer security*
- *Online vendor security*
- *Instant and pull-tab ticket security*
- *Locating instant and pull-tab tickets*
- *Computer security*
- *Data communications*
- *Database security*
- *System security*
- *Physical security*
- *Distribution security*
- *Validation and payment*
- *Unclaimed prizes*
- *Ticket counterfeiting and alterations*

The Lottery's overall security is very satisfactory, but several areas need improvements. As provided for under the Kansas Open Records Act, this public report only identifies areas where there are findings. A confidential report provides detailed findings and recommendations.

.....page 3

This audit was conducted by Delehanty Consulting, LLC, a firm under contract with the Legislative Division of Post Audit. If you need any additional information about the audit's findings, please contact Randy Tongier at the Division's offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@lpa.state.ks.us.

Final Report
Public Report
December 2007

Performance Audit of Security in the Operation of the Kansas Lottery

A Report to the
Kansas Legislative Post Audit Committee

Delehanty Consulting LLC
Security, Integrity, Performance

Table of Contents

PART 1: INTRODUCTION AND SUMMARY.....	1
Purpose	2
Objectives	2
Methodology.....	2
Summary of Findings	3
PART 2: EVALUATION AND FINDINGS.....	4
1.1 Organizational Scan.....	5
1.2 Personnel Security	5
1.3 Retailer Security	6
1.4 Online Vendor Security	6
1.5 Instant and Pull-tab Ticket Security.....	7
1.6 Locating Instant and Pull-tab Tickets	7
1.7 Computer Security	8
1.8 Data Communications	8
1.9 Database Security	8
1.10 System Security	8
1.11 Physical Security	9
1.12 Distribution Security.....	10
1.13 Validation and Payment.....	10
1.14 Unclaimed Prizes	10
1.15 Ticket Counterfeiting.....	10
1.16 Review of Previous Findings.....	11
1.17 Recommendations for Future Audits	11

PART 1: INTRODUCTION AND SUMMARY

Purpose

Delehanty Consulting LLC conducted a comprehensive lottery security audit of the facilities, operations, systems, games, policies, and procedures for the Kansas Lottery. An organizational meeting was held on October 9, 2007 with representatives from the Kansas Lottery, Kansas Legislative Division of Post Audit, and Delehanty Consulting. Field work began on October 9, 2007 and was completed on October 26, 2007. This audit was performed to meet the requirements of K.S.A.. 74-8707(b) and was conducted in accordance with the invitation for bids issued June 20, 2007.

The contents of this document are intended solely for the purpose of providing information to the Kansas Legislative Division of Post Audit, the Kansas Lottery and any of its subcontractors or state agencies the Lottery or the Legislative Division of Post Audit deems appropriate.

Objectives

The performance audit's overall objective was to perform an assessment of the security established by management to ensure the security, integrity, honesty, and fairness of the Kansas Lottery operations and games. The audit was performed in accordance with generally accepted government audit standards .

The lottery security audit did not include a review of the state's internal accounting controls, procedures, and financial reporting. The audit included a review of the physical controls, systems, and processes in place at the Great Bend regional office. The audit did not include a review of the sales or cashing activities performed by Lottery retailers.

Methodology

To accomplish these objectives Delehanty Consulting LLC used the following approach:

- Reviewed various documents and information to gain an understanding of Kansas nuances of critical lottery processes
- Met with Kansas Lottery management to clarify issues and to understand Kansas Lottery management's priorities and any special concerns
- Surveyed lottery and vendor employees to verify compliance with controls and to identify known and suspected risk areas
- Interviewed key Lottery and vendor personnel
- Verified the existence and effectiveness of the controls and processes in place to meet the Lottery's security objectives
- Identified weaknesses and associated risks
- Provided draft report to the Kansas Lottery for review and comment
- Completed report

The primary focus of the work effort was on high-risk areas based upon the input from the Kansas Lottery management team and upon our experience in the lottery industry.

Summary of Findings

Our review indicated the overall security of the Kansas Lottery is exceptional. The results of our organizational scan indicated a very strong security culture within the organization. Employees believe that management sets a strong tone on the importance of security and believe that security measures are consistently applied throughout the organization. More than 95% of the employees have confidence, trust, and respect in the Lottery management team. Every Kansas Lottery employee supports the Lottery's security program.¹

The Kansas Lottery's security culture may set the standard for the U.S. lottery industry. When compared with survey results from three other lottery jurisdictions, the Kansas Lottery results were the best in 10 of 21 categories.

Most procedures and systems are very sound and appear to be strictly adhered to by the Lottery staff. We found all practices appear to be in strict compliance with the Lottery laws.

During the review we identified 31 security related issues. Each issue was assigned a *High*, *Medium*, or *Low* risk level based on the likelihood and consequences of an occurrence of the risk. There were no High, seven Medium, and twenty-four Low risk issues.

¹ No employees indicated they would be unlikely to report a known or suspected security issue or security violation .

PART 2: EVALUATION AND FINDINGS

1.1 Organizational Scan

We began our audit with an Organizational Scan to assess the risks, determine priorities, and understand the existing Kansas Lottery culture as it relates to security. The scan included an exercise with the Kansas Lottery's senior staff and two employee surveys to elicit information that was used during the audit.

The results of the organizational scan indicated a very strong security culture within the organization. Employees believe that management sets a strong tone on the importance of security and believe that security measures are consistently applied throughout the organization. More than 95% of the employees have confidence, trust, and respect in the Lottery management team.

The Kansas Lottery's security culture may set the standard for the U.S. lottery industry. When compared with survey results from three other lottery jurisdictions, the Kansas Lottery results were the best in 10 of 21 categories. Only in response to a question regarding the ease of providing input on security issues did the Kansas Lottery employees provide a less favorable response than the three other lotteries.

1.2 Personnel Security

We reviewed the Lottery's policies, procedures, and practices regarding personnel. This included pre-employment procedures, terms of employment, post-employment procedures, and threats to employees. The Lottery's employees have significant confidence, trust, and respect in management. Employees believe that security measures are consistently applied and believe management sets a strong tone on the importance of security. The Lottery places significant emphasis on the safety of its employees.

The Lottery recognizes two categories of employees for the purposes of background investigations: 1) executive director and security enforcement personnel and 2) all other employees.

We reviewed the policies and procedures for performing initial background investigations for potential lottery employees, contractors and contractor personnel. Background investigations for these categories of individuals are performed by the Kansas Lottery, Security Division, Enforcement agents. These background investigations are exceptional in scope and thoroughness.

Our findings and recommendations to enhance security in this area encompassed three general areas:

- o Terms of employment as they relate to security and integrity
- o Security awareness and training
- o Background investigations of service providers who are not contractors

1.3 Retailer Security

Retailer management and retailer data are controlled by the Kansas Lottery. Policies, procedures, and practices used to manage retailers and retailer data are sound. Retailer application and Lottery approval process are in line with industry best practices and are closely followed.

Retailer backgrounds are required per K.S.A. 74-8705(c). The statute does not define the substance of the background. The substance of the background is defined in the Security Standards Handbook (Revised September, 2007). A review of a completed retailer background disclosed that the retailer's criminal history and motor vehicle records are checked. For small businesses, the owner would be checked while for a large corporate retailer, the corporate point of contact would be the subject of the background.

The Kansas Lottery's experience with retailer security has been commendable. Only 66 cases of alleged retailer violations have been reported during the past 11 years. Only two of these cases involved retailer fraud. Lottery Security performs retailer inspections when time is available; in recent years, the number of inspections has dropped from 900 per year to 300. The Lottery policies and practices regarding retailers are consistent with industry standards. New retailers receive training from the Kansas Lottery prior to beginning sales.

Our findings and recommendations to enhance security in this area encompassed one general area:

- o Initial retailer training

1.4 Online Vendor Security

We reviewed access controls in place for the Kansas Lottery and are hosted by GTECH to ensure access to sensitive data was only available to appropriate persons. There are two computer systems that are integrated to provide the functionality for the games. We conducted a 100% audit of persons with access to the GEMS front end system (left-hand side of the diagram) and identified no idle, unused, or aberrant user accounts. Group/role-based access is used. This is an industry best practice.

We reviewed GTECH's operational procedures and reviewed all incidents that occurred within the past three years. We found GTECH's operations to be very stable and relatively few incidents of operator errors. Although the systems deployed at GTECH are old by IT-industry standards, there are very few incidents of hardware failure. These systems are scheduled to be replaced within the next year.

We evaluated the overall network infrastructure for security controls and prudent design. This audit included the configuration of network devices through the tracing of selected critical wiring. The dominant feature is that there are actually two separate networks within the GTECH environment for the Kansas Lottery. One network is tightly controlled and used for gaming systems; called the Production network. The other network is for more general office use, such

as e-mail and other general office functions. The goal is to isolate gaming, high risk activity to the Production network.

Strengths of the production network include a robust and segregated design, equipment that is highly regarded in the industry, and administration by knowledgeable staff at GTECH corporate offices.

We performed a detailed review of GTECH's facility located at 128 N. Kansas Ave, Topeka, Kansas. Specifically, we reviewed the general offices, the QA room, and the computer operations room. The protective and monitoring practices and devices located in all areas meet the security requirements posed by the associated risks. Security monitoring is provided and controlled by the Kansas Lottery Security Division.

Our findings and recommendations to enhance security in online vendor security area encompassed four general areas:

- o Disclosure; Security Awareness and Training—GTECH
- o Access rights
- o Infrastructure monitoring and testing
- o Data processing equipment environmental controls

1.5 Instant and Pull-tab Ticket Security

We reviewed the security features and processes related to instant tickets and pull-tabs. The security features required by the Kansas Lottery and supplied by its vendors are consistent with best practices in the lottery industry. We also reviewed the instant ticket RFP and proposal that resulted in the 2001 contract with Pollard Banknote.

Our findings and recommendations to enhance security in this area encompassed two general areas:

- o Quality assurance
- o Third-party agreement for pull-tabs

1.6 Locating Instant and Pull-tab Tickets

We reviewed the Lottery's process for the reconstruction of instant tickets. We also reviewed the security requirements in the Instant Ticket RFP, Pollards' Proposal, and working papers for a pull-tab game.

The Lottery's processes for controlling the information required by employees to determine the location of prizes in pre-printed tickets are very sound. We reviewed the RFPs, proposals, and working papers but did not find sufficient information to determine whether the ticket vendors have sufficient controls in place to prevent vendor employees from obtaining enough information that they could collude with a lottery employee to locate pre-printed winning tickets.

1.7 Computer Security

We reviewed the access and control attributes in place to protect the information systems supporting the Lottery. Our review included attributes that could affect the availability, integrity, and confidentiality of the systems and system information.

Overall, we find that the determination of access rights for Kansas Lottery staff, and the procedures to administer these rights, is very well designed and executed. Our audit focused on the core systems within the Production network; especially ACCLAIMS.

We conducted both an overall scan of user accounts for appropriateness and zoomed in for detailed analysis on approximately ten (10) accounts. In all cases, access rights appeared appropriate for the role of the lottery staff. Furthermore, there are processes for an annual review of access rights and ongoing audits by a different staff person of changes to the systems.

Our findings and recommendations to enhance security in this area encompassed one general area:

- o Information classification

1.8 Data Communications

Our audit included an analysis of the general network design, configuration of key components, and the physical wiring for selected and critical areas. This section of the report relates to the network systems operated by the Kansas Lottery.

Our findings and recommendations to enhance security in this area encompassed two general areas:

- o Monitoring
- o Documentation

1.9 Database Security

We reviewed the controls in place to limit the access to sensitive data. The controls limit access to only authorized individuals and limits the access those individuals have to the type and level of access necessary to perform their job functions.

Our review in this area included an evaluation of the databases determined to be sensitive by the lottery. Database access is controlled and authorized by the Director of Enterprise Security. Database schema and file maintenance are performed by the IT staff. We sampled the level and types of access for employees and found all access to be consistent with sound security practices.

1.10 System Security

The Kansas Lottery has developed a Disaster Recovery Plan and has made significant progress in enhancing its disaster recovery capabilities by adding an offsite hot backup for its AS400 and its business file servers. Additionally, the new contract with the online gaming system provider requires the provider to have an offsite hot backup system.

Our findings and recommendations to enhance security in this area encompassed four general areas:

- o Documentation of application code
- o Documentation of software development lifecycle
- o Configuration management
- o Disaster recovery and business continuity.

1.11 Physical Security

Delehanty Consulting LLC performed an audit to evaluate the existence of, effectiveness of, and adherence to access and monitoring controls. We reviewed the security access levels for employees and performed a review of these facilities:

- Lottery Division Headquarters, 128 N. Kansas Avenue, Topeka, KS
- Lottery Warehouse, 128 N. Kansas Avenue, Topeka, KS
- Great Bend Regional Office, 3007 10th Street, Great Bend, KS
- GTECH Data Center Office, 128 N. Kansas Avenue, Topeka, KS

We reviewed the security features on the ground floor of the building at 128 N. Kansas Avenue, Topeka, KS. The protective and monitoring practices and devices located in the portions of the building reviewed meet the security requirements posed by the associated risks.

We performed a detailed review of the Lottery's Headquarter facilities located within the 128 N. Kansas Avenue facility. Specifically, we reviewed the general lottery offices on the 2nd floor, the Security Office, the Lottery Mail Room, and the Validations area. The protective and monitoring practices and devices located in the lottery areas meet the security requirements posed by the associated risks.

We performed a review of the Lottery's warehouse facility co-located at 128 N. Kansas Avenue, Topeka, KS. The protective and monitoring practices and devices located on, and within, the building meet the security requirements posed by the associated risks

We performed a review of the Great Bend Regional Office at 3007 10th Street, Great Bend, KS. The building is locked during non-business hours and cleaning staff with keys have access to building after hours. The space is alarmed after hours with response by the local police department and Lottery Security.

We reviewed the Lottery's Asset Management processes and performed a sampling of the documented inventory.

Our findings and recommendations to enhance security in the physical security and asset management area encompassed three general areas:

- o Segregation and protection of critical equipment and devices

- o Service and change documentation
- o Policy and practice alignment for asset management

1.12 Distribution Security

We reviewed the processes and procedures for distributing instant tickets between lottery locations and to retailers. We also reviewed the processes for ticket returns. The Lottery's procedures and systems are sound and appear to be strictly adhered to by the staff. We did not review the physical security controls provided while tickets are in the possession of FedEx. Our findings and recommendations to enhance security in the area of distribution security encompassed two general areas:

- o Documentation
- o Periodic inventories

1.13 Validation and Payment

We reviewed the physical systems and administrative procedures for handling ticket claims at the Lottery Headquarters. This included a detailed review of mailroom processing, Security processing and Finance processing. The procedures were sound and appear to be adhered to by the staff.

1.14 Unclaimed Prizes

We reviewed the ability of GTECH Computer Gaming System and processes to guard against the ability for Lottery or vendor employees to fraudulently cash unclaimed prizes. The Lottery's policies and procedures for protecting unclaimed prizes of \$5,000 or more represent industry best practices. Our findings and recommendations to enhance security in the area of unclaimed prizes encompassed one area:

- o Protection of unclaimed prizes under \$600

1.15 Ticket Counterfeiting

Our reviews of the online vendor security in Section 1.4 and of the instant and pull-tab security in sections 1.5 and 1.6 included assessments of the ability for perpetrators to successfully counterfeit tickets. Our review of the validation and payment process in section 1.13 included an assessment of the ability for individuals to alter claim forms and to submit false claims.

In addition to the reviews discussed above, we also reviewed the Lottery Security database that contains records of all security issues reported to the Lottery. Based upon our review and assessment, the Kansas Lottery is providing adequate security against all known, economically viable counterfeiting techniques. Furthermore, Lottery Security's response to suspicious activity is excellent.

1.16 Review of Previous Findings

We conducted a detailed review of the findings from the 2004 audit. Three previous findings had not been corrected prior to the beginning of our field work.

- o Software quality assurance
- o Security awareness and training program
- o Penetration testing

1.17 Recommendations for Future Audits

The scope of the performance audit required by the Request For Proposals did not include a number of areas that are sometimes included in third-party lottery security audits and evaluations. The Kansas Legislative Post-Audit Division and the Kansas Lottery may want to consider including these items in future performance audits.

- o Lottery drawings and drawing processes including random number generators and second chance drawings
- o Compliance with ADA requirements
- o Security of instant and pull-tab tickets during the vendors' programming and manufacturing processes
- o Online vendor's warehouse security
- o Online vendor's ticket stock procurement, inventory, shipping, and receiving processes
- o Lottery purchasing and contract management processes
- o Governance –with respect to the Lottery's interaction with the Kansas Lottery Commission and with respect to the Commission's functions and performance
- o Security of electronic instant tickets
- o Instant ticket reconstruction process used by the Instant Ticket Vendors.
- o State Fair drawings or other special drawings