## Contents

1 Executive Summary

1.1 Overall Summary

1.1.1 CSL Security Process Strengths

1.1.2 CSL Security Process Opportunities for Improvement

1.2 Background and Purpose

1.3 Scope and Approach

1.3.1 Scope of Security and Controls Assessment

1.3.2 Methodology Performed for the Security and Controls Assessment

1.3.2.1 Planning

1.3.2.2 Discovery

1.3.2.3 Assessment

1.3.2.4 Reporting

2 Security and Controls Assessment Results (CSL Lottery Act Areas)

2.1 Computer Security

2.2 Data Communications Security

2.3 Database Security

2.4 Security Control and Physical Security

2.5 Personnel Security

2.6 Lottery Game Retailer Security

2.7 Contractor Security (Third Party/Vendor)

2.8 Manufacturing Operations Security

2.9 Security against Ticket Counterfeiting, Alterations, and Fraudulent Winning

2.10 Security in Drawings

2.11 Security in Distribution

2.12 Validation and Payment Security

2.13 Unclaimed Prizes Security

2.14 Particular Game Security

2.15 Security against Locating Winners for Games Having Preprinted Winners

2.16 Other Aspects of Security Applicable to the Lottery and its Operations
1 Executive Summary

1.1 Overall Summary

The California State Lottery (CSL) was created by the California State Lottery Act of 1984 (Lottery Act), which established the CSL as an independent State commission to market and sell lottery products to the California State (State) public. Section 8880.46 of the California Government Code requires an independent audit of the CSL’s security to be performed bi-annually. KPMG LLP was contracted to perform a Risk Assessment and Security Audit (RASA), which includes a security risk assessment and audit of security related controls that mitigate significant CSL security related risks. The results of the security risk assessment, completed in October 2009, provided input for determining where to focus efforts in evaluating control processes that mitigate significant risks to the achievement of key CSL objectives.

During the Security and Controls Assessment phase, which this report represents, we developed an understanding of the security control processes for mitigating CSL risks. This detailed understanding enabled KPMG to further assess and determine if security controls identified during the risk assessment phase are integrated into CSL business and technical processes. The Security and Controls Assessment report includes the results of the Security Audit. The results stated in this report are categorized by the sixteen scope areas defined in Section 8880.46 of the government code.

1.1.1 CSL Security Process Strengths

In assessing the CSL’s security processes in further detail as part of the Security and Controls Assessment, we found the following overall security process strengths including, but not limited to the following:

- Overall, the CSL has repeatable processes as they relate to Information Technology supporting CSL operations and business requirements, although we have identified opportunities for improving the CSL’s overall security posture.

- There is a strong commitment to protecting physical assets at the CSL headquarters and other facilities with security guards and regular security inspections of physical access controls. Physical access for new employees are approved, and revoked upon separation on a timely basis.

- Key CSL operations outsourced to GTECH Corporation, a third-party vendor, have managed control processes that are subject to an annual Statement on Auditing Standards (SAS) No. 70, Service Organizations,
audit. CSL and GTECH managed processes include user access management, change management, and incident security management.

- System changes are reviewed by GTECH and CSL. Key CSL system changes related to new games and promotions are approved and tested prior to migration into the production environment.
- Personnel background checks are conducted for all employees, contractors and third party vendors (including all GTECH personnel). In addition, access granted to CSL systems is approved on a timely basis.
- Human Resources have initiated various projects related to workforce succession planning and new employee training that is focused on CSL products in general. Additionally, the CSL has been actively managing other State of California workforce matters including efforts to fill vacant personnel positions and the reduced State work schedule due to required personnel furlough days.
- CSL has documented a detailed Operational Recovery Plan.
- CSL has incorporated anti-fraud and integrity checks into the CSL operations, such as processes around fraudulent ticket and fraudulent claims detection.
- Criminal and financial background checks are performed of CSL retailer applicants.
- CSL processes to review and approve access to the GTECH system are in place.
- An independent evaluation of ticket manufacturer security controls with potential impacts to CSL was performed in 2009.
- CSL gaming product contractors undergo routine independent reviews and security controls assessments.
- Independent auditors participate in routine key draw activities and attest to agreed upon draw procedures, including the validation of CSL draw results.
- CSL claims processing is a mature operation supported by comprehensive and detailed policy and procedures.
- Segregation of duties appears to exist within the CSL’s key operations.

### 1.1.2 CSL Security Process Opportunities for Improvement

The following is a summarized listing of areas that would benefit from additional security processes and controls to help strengthen the CSL’s overall security posture:

- Information Security governance processes
- Security training and awareness programs
• System user access termination and management processes
• Third party vendor security assessments
• Processes for managing and classifying assets containing sensitive and confidential information
• Processes for accessing CSL systems and network devices
• Processes for monitoring computing devices for security vulnerabilities and access to the CSL computing infrastructure
• Processes for managing security incidents
• Information asset disposal processes
• Game player access to winning ticket information
• End of Scratcher game processes
• Physical security over the Make Me a Millionaire game show
• Draw management and Draw related game policies and procedures
• Processes to help ensure accurate Scratcher ticket product order processing and distribution
• Processes to further secure Scratcher game tickets from inappropriate knowledge of winning ticket locations

The CSL has recently appointed a full time Information Security Officer. Having filled this role, the CSL is now in a better position to establish improved policy, guidelines, procedures and enforcement practices to help ensure that the CSL’s systems, data, and asset protection efforts are consistently understood and applied across the enterprise and that improved controls implemented at the CSL help prevent unauthorized access to or loss of the CSL’s assets.

1.2 Background and Purpose

The CSL was created by the California State Lottery Act of 1984 (Act), which established CSL as an independent State commission to market and sell lottery products to the California State (State) public. Section 8880.46 of the California Government Code requires an independent audit of CSL Security to be performed bi-annually. KPMG LLP was contracted to perform the RASA, which is comprised of a security risk assessment and audit of security related controls that mitigate significant CSL risk. This report includes the results of the Security and Controls Assessment or Security Audit. The results of the first phase of RASA, which was the October 2009 risk assessment, should assist CSL Internal Audit and other CSL management, responsible for implementing and managing security processes, to better understand significant risks that potentially impact the achievement of CSL objectives, and the processes in place to mitigate the risks. The risk assessment effort served as the foundation for the security and controls evaluation.
CSL’s goals and objectives are supported by its mission to service California’s mandate to maximize supplemental funding for public education. The CSL leverages the responsible sale of lottery products to achieve this mission. Key CSL operational processes and activities that support the sale of these products include the design of lottery gaming products, use of third parties and retailers to support CSL operations and sales, and the payment of prize winners.

In order to achieve its mission, the CSL must protect its critical assets such that the CSL can achieve its maximum potential of funding State education needs. CSL assets are more than physical items of economic value and include intangible organizational property such as gaming product intellectual property, brand and reputation, sensitive employee information or prize winner data stored on key systems. CSL awareness of the need to protect its critical assets will help ensure that key objectives are achieved. The CSL has acknowledged the importance of security over critical assets by engaging KPMG to perform this Risk Assessment and Security Audit.

Additionally, the CSL was founded on the principles of integrity, security, honesty and fairness. In every product sold, and every communication developed, for every marketing scheme developed, upholding the public’s trust is the cornerstone for which these activities are created, designed and deployed. While the general public knows the CSL commonly through its retailers and game products, most are not aware of the high level of vigilance devoted to maintaining the integrity, security, honesty and fairness that translates into public trust and confidence in the games and products of the CSL.

1.3 Scope and Approach

The California State Lottery Act\(^1\) specifies both general IT areas as well as specific Lottery Operational areas to be reviewed as part of the bi-annual security audit. The scope of this report, the Security and Controls Assessment, includes the results of our review of security related controls that mitigate high rated risks identified during the risk assessment. The in-scope areas are noted in Table 3.

---
\(^1\) California Government Code 8880 Section 46 (The Lottery Act)
<table>
<thead>
<tr>
<th>Lottery Act Security Areas</th>
<th>Other Areas included in the Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lottery Game Retailer Security</td>
<td>Workforce Management</td>
</tr>
<tr>
<td>Contractor Security (Third Party/Vendor)</td>
<td>Segregation of Duties</td>
</tr>
<tr>
<td>Manufacturing Operations Security of Lottery Contractors</td>
<td>Outsourced Functions</td>
</tr>
<tr>
<td>Security Against Ticket Counterfeiting and Alterations and Fraudulent Winning Prevention</td>
<td></td>
</tr>
<tr>
<td>Security of Drawings</td>
<td></td>
</tr>
<tr>
<td>Security in Distribution</td>
<td></td>
</tr>
<tr>
<td>Validation and Payment Security</td>
<td></td>
</tr>
<tr>
<td>Unclaimed Prizes Security</td>
<td></td>
</tr>
<tr>
<td>Locating Preprinted Winners Games Security</td>
<td></td>
</tr>
<tr>
<td>Particular Game Security</td>
<td></td>
</tr>
<tr>
<td>Computer Security</td>
<td></td>
</tr>
<tr>
<td>Security Controls and Physical Security</td>
<td></td>
</tr>
<tr>
<td>Data Communications</td>
<td></td>
</tr>
<tr>
<td>Personnel Security</td>
<td></td>
</tr>
<tr>
<td>Database Security</td>
<td></td>
</tr>
</tbody>
</table>

KPMG’s Security and Controls assessment of security risks in the CSL organization relied on and was guided by industry standards and State of California regulations and guidelines, reflected below in Table 4. The KPMG Security and Controls Assessment analysis and conclusions are based on data gathered from the interviews and review of documentation that supports many of the CSL’s key processes.

The items listed in Table 4 are not an exhaustive list of all standards that might be applicable for this type of assessment. These standards contain some degree of overlap with each other, are not listed in any particular priority, and only represent the general framework to KPMG’s work approach.
KPMG’s approach for the RASA Project followed the Enterprise Risk Management (ERM) Methodology that was designed to help formulate detailed risk profiles that can be used to refine and improve risk management strategies. For the CSL, KPMG’s ERM methodology and approach:

- Incorporates management’s perceptions, assumptions, and judgments about the CSL’s security risks and controls and their potential impact on the agency.
- Focuses on those risks identified as potential security and non-security exposures discovered during the interviews with process owners and review of documents supporting leading industry better practices.
- Produces a list of potential security risks within the enterprise areas under review, including identification of mitigation activities and additional considerations that might improve the effectiveness of internal controls within existing processes to mitigate these risks.

### 1.3.1 Scope of Security and Controls Assessment

For the 2009 Security Audit, the CSL requested a comprehensive study of the CSL’s security related risks and mitigation strategies in place for minimizing the impact of events that may prevent the CSL from achieving its overall objectives. The scope of work to accomplish the objectives of the project includes:

- Identify vital components of the CSL’s operations;
- Assess each component to determine its dependency on other components and the associated risk to the CSL;
- Identify from this work those areas that represent highest risk to the CSL;

<table>
<thead>
<tr>
<th>Standard</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>International Organization for Standardization : 27002</strong></td>
<td>Leading Information Security management practices</td>
</tr>
<tr>
<td><strong>California State Administrative Manual 5305</strong></td>
<td>California State Information Security leading practices guidance</td>
</tr>
<tr>
<td><strong>World Lottery Association</strong></td>
<td>Leading lottery operational and security practices</td>
</tr>
<tr>
<td><strong>California Lottery Act</strong></td>
<td>Required areas for bi-annual security review</td>
</tr>
<tr>
<td><strong>COSO Enterprise Risk Management Framework</strong></td>
<td>Enterprise Risk Management framework</td>
</tr>
</tbody>
</table>
Perform both general and internal control evaluations of security related processes associated with areas of high risk to the CSL; and

Perform technical and operational reviews of the areas identified in the California Lottery Act.

The California State Lottery Act\(^2\) specifies both IT related areas as well as specific CSL Operational areas required to be reviewed as part of the bi-annual security audit. The scope of this report encompasses risks mitigated by security.

**1.3.2 Methodology Performed for the Security and Controls Assessment**

KPMG employed the following phased approach for conducting the assessment of CSL Security and Controls. Each phase of the assessment led to the next segment and leveraged work performed in all prior segments, while applying a structured project management methodology.

The assessment consisted of four phases, including:

- **Phase I – Planning:** Development of Project Management Plan and Tools. The Planning phase is described further below.

- **Phase II – Discovery:** Information Collection, Validation, and Development of Initial Findings. During this phase, the CSL Risk Assessment was conducted. The Risk Assessment process incorporated a review of the CSL’s risk environment as well as identification of controls that mitigate the risks. The risks and controls “discovered” during this phase provided the foundation for a more comprehensive review of mitigating controls performed in the subsequent Assessment phase. The Discovery phase is described further below.

- **KPMG provided risk mitigation considerations for process improvement to the CSL during this phase. These risk mitigation strategies were further reviewed during the Assessment phase and are addressed in the Security and Controls Assessment Results section in this report.**

- **Phase III – Assessment:** Detailed Analysis and Development of Findings and Recommendations. During this phase, CSL risks dependent on security controls were reviewed and summarized. The sample of risks and related controls reviewed during the Assessment phase was based on the results of the Risk Assessment and the risk rating assigned to individual risk items. The sample reviewed during the Assessment phase included controls associated with Critical and High level risk items. The Assessment phase is described further below.

\(^2\) California Government Code 8880 Section 46 (The Lottery Act)
• Phase IV – Reporting: Compilation and Summarization of Findings and Recommendations, Follow-Up Activities. During this phase, the assessment of data from Phase II and III were finalized and summarized. The Reporting phase is described further below.

1.3.2.1 Planning

KPMG met with the Project Sponsor (CSL’s Internal Audit Chief) and confirmed the Security Assessment scope and timing, established project milestones, discussed expectations and assigned responsibilities. In addition, we identified automated tools to be utilized throughout the assessment, identified key stakeholders and developed an initial schedule of interviews and meetings.

1.3.2.2 Discovery

KPMG conducted interviews, observed current security processes and obtained and reviewed pertinent CSL documentation. KPMG also identified and documented pertinent Federal and State statutes and regulations, leading practices, and industry standards. The deliverables from this phase was a Risk Assessment Report and Risk Register delivered to the CSL in October 2009.

1.3.2.3 Assessment

Based on Phases I and II, KPMG performed a Security and Controls Assessment. During the course of this phase of the project the following were performed:

• Inspected and assessed documentation including: security policies and procedures, process documentation, prior reports and third party reviews

• Randomly selected and inspected representative samples to confirm the existence of controls to mitigate CSL risks

• Observed key processes and operations

• Performed inquiry of key personnel to enhance understanding of CSL processes

• Assessed processes and controls associated with the CSL’s personal, sensitive, and confidential data and information resources identified during the risk assessment

• Communicated significant concerns to the CSL Project Manager as they were identified, and performed additional analysis as required

• Periodically met with CSL Division management to provide progress updates and communicate preliminary findings.
1.3.2.4 Reporting

KPMG has documented the results from our review and analysis of security processes and documentation in the Security and Controls Assessment report. KPMG also reported weekly status to the CSL Project Manager and held meetings with other key CSL stakeholders on a regular basis. Information on pertinent security risks and vulnerabilities and their potential impact to the CSL was communicated in the weekly status updates and meetings with key stakeholders.
2 Security and Controls Assessment Results (CSL Lottery Act Areas)

This section contains the results from the CSL Security and Controls assessment. Each subsection below corresponds to the sixteen CSL Lottery Act areas. A description of the subsection is provided as well as our high level recommendations for improvement.

2.1 Computer Security


Based on the review of CSL Computer Security, KPMG determined that this area has a **High** overall risk rating. Overall, the CSL has repeatable processes as they relate to Information Technology supporting CSL operations and business requirements. However, we have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Security policies including Information Security standards, procedures, and baseline requirements
- Information Security Committee Charter and continuous risk assessment process
- Processes for classifying sensitive and confidential information
- Processes for managing and tracking computing assets
- Processes for managing and tracking security incidents
- Processes for periodic testing and updating the CSL Business Continuity and Operational Recovery Plan
- Processes for monitoring compliance with security policies and standards

2.2 Data Communications Security

The Data Communications Security subsection includes information on the CSL’s security controls related to Communications and Operations Management and Network logical access.

Per ISO 27002, the key objectives of Data Communications Security are:
To help ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes developing operating procedures related to the availability of adequate capacity and resources, preventing and detecting malicious code, taking back-up copies of data and rehearsing their timely restoration, managing secure networks, preventing unauthorized disclosure, modification, removal or destruction of assets and detecting unauthorized information processing activities.

To control access to information. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take into account policies for information dissemination and authorization.

To prevent unauthorized access to networked services. Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services by establishing authentication mechanisms for users and equipment as well as control over user access to information services.

To prevent unauthorized access to operating systems. Security should be used to restrict access to operating systems to authorized users. Security should be capable of the following: a) authenticating authorized users, in accordance with a defined access control policy; b) recording successful and failed system authentication attempts; c) recording the use of special system privileges; d) issuing alarms when system security policies are breached; e) providing appropriate means for authentication; f) where appropriate, restricting the connection time of users.

Based on the review of CSL Data Communication Security, KPMG determined that this area has a **High** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Network device authentication controls
- Mobile Device and Removable Media policy and procedures
- Processes for restricting access to information in connection with media that has been disposed
- Processes for allowing privileged and regular user network and system access
- Logon password controls
- Security configuration hardening standards and processes
- Network and system scanning and monitoring processes
• Data back-up and business resumption procedures
• Microsoft Windows server and desktop patching processes
• Processes for restricting vulnerable system communication protocols

2.3 Database Security

This subsection includes CSL security controls related to Information System Acquisition, Development & Maintenance, and database logical access.

Per ISO 27002, the key objectives of this section are:

• To prevent unauthorized access to information held in application systems. Security facilities should be used to restrict access to and within application systems. Logical access to application software and information should be restricted to authorized users. Application systems should: a) control user access to information and application system functions, in accordance with a defined access control policy; b) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls; c) not compromise other systems with which information resources are shared.

• To help ensure that security is an integral part of information systems. Security requirements should be identified and agreed prior to the development and/or implementation of information systems. All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

Based on the review of CSL Database Security, KPMG determined that this area has a High overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

• Database encryption processes
• Processes for privileged access to the database server environment
• Database logging and auditing processes

2.4 Security Control and Physical Security

This subsection includes CSL’s security controls related to the Physical and Environmental Security.

Per ISO 27002, the key objectives of this section are:

• To prevent unauthorized physical access, damage, and interference to the organization’s premises and information. Critical or sensitive information
processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.

- To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities. Equipment and data should be protected from physical and environmental threats.

Based on the review of CSL Security Control and Physical Security, KPMG determined that this area has a **Medium** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Physical access key management processes

### 2.5 Personnel Security

This subsection includes CSL’s security controls that relate to Human Resource functions supporting CSL business operations.

Per ISO 27002, the key objectives of this section are:

- To help ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

- To help ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

- To help ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

Based on the review of CSL Personnel Security, KPMG determined that this area has a **Medium** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Security awareness and training processes
- Processes to help ensure employee acknowledgement of CSL Information Security policies and procedures

### 2.6 Lottery Game Retailer Security

The CSL game retailer security includes the security environment to appropriately establish, maintain and monitor retailer relationships to help ensure proper retailer integrity and asset protection. This area focuses on key controls associated with the
standard retailer contract, training and incidents involving retailers. This area also includes game close out activity to help ensure retired Scratcher games are not sold by retailers.

Based on the review of CSL Lottery Game Retailer Security, KPMG determined that this area has a **High** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Security incident report processes
- Game player access to winning ticket information
- End of Scratcher game processes

### 2.7 Contractor Security (Third Party/Vendor)

Per ISO 27002, the key objective of Third Party Security is to maintain the security of the organization’s information and information processing facilities so that they are accessed, processed, communicated to, or managed by external parties. The vendors addressed in this section provide outsourced gaming operations services. Vendors related to ticket manufacturing are addressed in the Manufacturing Operations Security section.

Based on the review of CSL Contractor Security, KPMG determined that this area has a **Medium** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following area:

- Third Party Vendor Security Assessment and Management processes

### 2.8 Manufacturing Operations Security

The CSL manufacturing security includes the security environment related to CSL contractors who provide critical CSL game manufacturing support. This area focuses on key controls associated with primary ticket manufacturer vendors, their contracts, and associated security measures. This area does not include critical gaming operations covered above in the Contractor Security area.

Based on the review of CSL Manufacturing Operations Security, KPMG determined area has a **Medium** overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following area:

- Training processes related to CSL scratcher game manufacturing
2.9 Security against Ticket Counterfeiting, Alterations, and Fraudulent Winning

The CSL ticket counterfeiting, alterations, and fraudulent winning security includes reviewing and monitoring of key physical game ticket security measures and gaming activities that help ensure game integrity. This area focuses on the design and physical integrity of gaming products that could be compromised and result in fraudulent claims and winnings.

This area does not include security measures performed on prize claims and questionable game tickets for validation or payment processing covered under the Validation and Payment Security area of the Lottery Act.

Based on the review of CSL Ticket Counterfeiting, Alterations, and Fraudulent Winning Security, KPMG determined this area has a Low overall risk rating. No findings or associated recommendations were identified in this area.

2.10 Security in Drawings

The CSL security in drawings includes the security environment that provides for proper draw activities and protection of draw game integrity. This area focuses on key controls associated with the conduct of “on-line” draw games including traditional periodic jackpot draw games, such as SuperLOTTO Plus, HotSpot, MEGA Millions; and daily draw games such as Daily 3, Daily 4, Daily Derby and Fantasy Five. This area also includes promotional related draws games, such as the Make Me A Millionaire game show and the Scratcher “replay” program. Control areas considered for review include draw related policies and procedures including emergency procedures, game approval, draw randomization and validation, physical access to draw facilities, and inspecting and maintaining draw appliances/equipment and ball sets.

Based on the review of CSL Security in Drawings, KPMG determined this area has a High overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following areas:

- Physical security over the Make Me a Millionaire game show
- Draw management policy and procedures

2.11 Security in Distribution

The CSL security in distribution includes the security environment that provides for the protection and accuracy of Scratcher gaming tickets in transit and in inventory to help ensure proper gaming protection and integrity. This area focuses on key controls associated with the secure transport, receipt, order processing, and shipping of Scratcher tickets to retailers.
Based on the review of CSL Security in Distribution, KPMG determined this area has a Medium overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following area:

- Processes to help ensure accurate Scratcher Ticket product order processing and distribution

2.12 Validation and Payment Security

The CSL validation and payment security includes the security environment that provides for secure claims processing and validation that help to ensure proper prize payment integrity. This area focuses on key controls associated with retailer and CSL personnel validating tickets, CSL flagging and investigating large prize winnings and suspicious claims and tickets, CSL authorization of claims for California State Controllers Office (SCO) payment, and the physical security over the CSL prize payment operations.

Based on the review of CSL Validation and Payment Security, KPMG determined this area has a Low overall risk rating. No findings or associated recommendations were identified in this area.

2.13 Unclaimed Prizes Security

The CSL unclaimed prize security includes the security environment that provides for secure funds to pay claimants for game prize winnings. This area focuses on key controls associated with dedicated game accounting, timely purchase of periodic investments and the monitoring of large and outstanding unclaimed prizes.

Based on the review of CSL Unclaimed Prizes Security, KPMG determined this area has a Low overall risk rating. No findings or associated recommendations were identified in this area.

2.14 Particular Game Security

The CSL particular game security includes the security environment over the various major game types including individual Scratcher games and draw related games including large jackpot games that help to ensure proper game integrity and asset protection. This area focuses on key controls associated with the on-line gaming and Scratcher product vendors, protection against gaming and product fraud and securing the appropriate funds to pay claimants. Specifically, this area includes security measures and processes that were considered when reviewing the major gaming types included in the other Lottery Act Areas of this report, for example, Contractor Security (Third Party/Vendor), Manufacturing Operations Security, Security against Ticket Counterfeiting, Alterations, and Fraudulent Winning, Security in Drawings, Security in Distribution, Unclaimed Prizes Security, and Security against Locating Winner for Games Having Preprinted Winners.
No findings or associated recommendations were identified in this area.

2.15 Security against Locating Winners for Games Having Preprinted Winners

The CSL security against locating winners for games having preprinted winners includes the security environment that provides measures to protect Scratcher products from dishonest game players seeking to gain an unfair game advantage and help to preserve the integrity of Scratcher games. This area focuses on the production design and physical integrity of gaming products that could be compromised and result in inappropriate exposure of winning ticket locations.

This area relates to but does not specifically include a focus on content covered in other Lottery Act Areas including: Manufacturing Operations Security and Security against Ticket Counterfeiting, Alterations, and Fraudulent Winning.

Based on the review of CSL security against locating winners for games having preprinted winners, KPMG determined this area has a Medium overall risk rating. We have identified opportunities for improving the CSL’s overall security posture and provided recommendations in the following area:

- Processes to secure Scratcher game tickets from inappropriate knowledge of winning ticket locations

2.16 Other Aspects of Security Applicable to the Lottery and its Operations

Other aspects of security applicable to the CSL and its operations may include security controls that protect CSL assets from loss or harm that are not already included in other areas of the Lottery Act.

KPMG’s review and observations of security related controls have been reflected in one of the other defined Lottery Act Areas of this report and therefore there are no additional findings for this section.
3 Additional Areas Reviewed

3.1 Workforce Management

This area includes KPMG’s high level assessment of the CSL’s workforce environment and related Human Resource management activity. Lottery’s workforce environment includes its staffing to support operations, Human Resource organization functions, and management’s roles and responsibilities in maintaining staffing to support workforce operations.

The CSL operations benefit from contracting much of its operations to third party vendors, including nearly all of its gaming operations and certain Sales and Marketing and facility operations. Considering the significant outsourcing at the CSL, staffing levels for CSL operations including Finance, Human Resources, and Information Technology, and Operations generally appear typical of State of California agencies and departments. Lottery Human Resource management has been actively managing common State of California workforce environment issues including efforts to fill vacant personnel positions, performance of succession planning and necessary adjustments to the reduced State work schedule and required personnel furlough days.

No additional findings or associated recommendations were identified in this area.

3.2 Segregation of Duties

KPMG performed a high level assessment of some of the CSL’s major operational areas, including CSL gaming operations, game product and claims processing activities and found the CSL segregation of duties to be satisfactory. Manual and system controls are in place to help enforce segregation of duties as determined through interviews and reviews of the CSL process documentation. Much of the CSL’s operations rely on third party systems and operational support, for example gaming and prize processing support provided by GTECH. Many of Lottery operational activities interface with these systems and support processes which provide for compensating controls. For example, claims processing and validation procedures require validation with the GTECH system before prizes can be authorized for payment.

Specifically, KPMG found that there is segregation of duties around CSL’s key gaming system, GTECH.

No additional findings or associated recommendations were identified in this area.
3.3 Outsource Functions – GTECH and Ticket Manufacturers

KPMG reviewed CSL’s major outsourcing contracts, including GTECH and key ticket manufacturers, and found that the terms of the contracts required or allowed CSL the right to audit its vendor’s operations and documentation. KPMG inspected CSL’s GTECH contract and found that annual independent audits are required of GTECH including internal control (SAS70) and financial audits. KPMG inspected the Scientific Games International (SGI) contract and found that in addition to CSL’s right to audit, additional independent reviews of instant game process are required of SGI. KPMG was informed that these independent reviews were being performed of CSL’s major ticket manufactures and these third party reports were being provided to CSL for periodic review.

No additional findings or associated recommendations were identified in this area.
4 Appendix A – Lottery Executive Response
February 24, 2010

Bryan Gillgrass, PMP  
Managing Director, Advisory Services  
KPMG LLP  
Suite 800  
400 Capitol Mall  
Sacramento, CA 95814

Subject: Biennial Security Audit

Dear Mr. Gillgrass:

The California State Lottery has set strategic goals that focus on continuous improvement of our products and enabling processes. As such, the CSL is committed to incorporating many industry leading practices identified throughout this audit in its operations. Thank you for your comprehensive and thorough assessment that will contribute to improvements in our processes and practices while helping to assure the public and players that California Lottery games are secure and fair.

The California Lottery agrees with your findings documented in this report and either has implemented or is in the process of implementing many of the recommendations. We appreciate your participation and identification of opportunities for improvement as well as your recommendations for best practices that the CSL can embrace.

Sincerely,

Joan M. Borucki  
Director