Security Assessment Report

Prepared for

California State Lottery

By:
Gaming Laboratories International, LLC.
600 Airport Road,
Lakewood, NJ 08701
Phone: (732) 942-3999
Fax: (732) 942-0043
www.gaminglabs.com

Audit Report	
Jurisdiction:	California
Document Reference:	California State Lottery Security Assessment Public Report
	Project OS-023-CLO-12-001
Classification:	Public
Revision Date:	February 11, 2013

Initially published and distributed on February 11, 2013.

Table of Contents

SECTION ONE: EXECUTIVE SUMMARY

OVERALL SUMMARY

The California State Lottery (CSL) was created by a 1984 ballot initiative. The portion of the initiative known as the California State Lottery Act of 1984, establishes the CSL as an independent state agency to market and sell lottery products to the California public. The California State Lottery Act of 1984 requires the Commission to engage an independent firm experienced in security procedures, including but not limited to computer security and systems security, to conduct a comprehensive review and evaluation of key aspects of security in the operation of the CSL. This security audit will follow-up on past concerns noted in previous audits, in addition to the requirements mandated by the Lottery Act of 1984 section 8880.46.

Gaming Laboratories International, LLC (GLI) was selected as the independent third-party security auditor. For nearly 25 years, GLI has been the world leader in providing independent testing, inspection and certification services to the gaming, wagering and lottery industry. With 20 laboratory locations located across Africa, Asia, Australia, the Caribbean, Europe, North America and South America, GLI is the only global organization of its kind to hold U.S. and international accreditations for compliance with ISO/IEC 17025, 17020 and guide 65 standards for technical competence in the gaming, wagering and lottery industries.

The overall purpose of this engagement was to conduct a comprehensive review of all aspects of lottery security in accordance with the Lottery Act of 1984, section 8880.46. The audit assessed the security measures that support the integrity, honesty and fairness of CSL's operations, computer security, and system security. Our assessment was conducted using a risk based methodology to determine security control risk by evaluating the criteria of likelihood and impact of the risk event occurring and was concluded December 2012.

GLI's audit plan was developed to fulfill the requirements of section 8880.46. GLI grouped these requirements logically to map back the various security control domains within the ISO 27001 Information Security Management Standard and World Lottery Associations Security Control Standard (WLASCS). Our team will utilize a standard industry based audit methodology for this engagement to gain a complete understanding of the lottery operation and the policies and procedures used to manage the business of gaming.

GLI has determined that CSL is compliant with the Lottery Act of 1984, section 8880.46 along with a number of opportunities for continual improvement. This audit report details the strengths of the CSL security processes and the high risk areas that have opportunities for improvement.

CSL SECURITY PROCESS STRENGTHS

During the assessment of CSL's information security controls covering Information Technology systems and gaming operations the following areas of strengths were identified:

- Overall, CSL and gaming vendors that support the Information Technology gaming environment provide mature standardized industry process.
- CSL's third-party vendor for gaming systems GTECH has developed a mature information security control environment that is subject to an annual SSAE16 audit. SSAE 16 is an enhancement to the current standard for Reporting on Controls at a Service Organization, the SAS70. GTECH's information security controls include the following standardized security domains; information security policy, organization of information security, asset management, human resource security, physical and environmental security, communications and operations management, access control, systems acquisition, development and maintenance, security incident management, and business continuity management.

- CSL has developed a strong commitment to the delivery of lottery games and have developed mature standardized gaming processes across Instant Ticket “Scratcher”, and Lottery Draw Games.
- CSL security controls are mature and have been established within the Instant Ticket “Scratcher” line of business covering; game design, ticket printing, shipment of tickets, storage and distribution of tickets, retailer security, ticket validation and game closure.
- CSL security controls have been established within the Lottery Draw line of business covering; lottery draw management, draw operations, draw audit and security of draw devices.
- The lottery also utilizes the services of a third-party audit firm to perform independant montoring and validation of all draw functions and procedures performed for lottery games.
- CSL has established a mature anit-fraud and integrity program for its lottery games.
- The lottery has developed processes for the protection of Prize Money that includes; winner validation and prize payout processes, as well as, process and system controls to protect unclaimed prize money.
- Processes have been established for the recruitment and set-up of retailers that include financial and security back ground checks.
- CSL has established a robust security investigation, quality assurance and monitoring program that cover third-party ticket printing vendors, as well as, distribution retailers.
- The lottery maintains the integrity of its operations by maintaining a strict segregation of duties across lottery functions including Infromation Technology, game design and winner selection.
- CSL’s information technology systems have developed an information security control environment that is subject to internal audits along with biennial security reviews by third-party vendors. CSL’s information security controls include the following standardized security domains; information security policy, organization of information security, asset management, human resource security, physical and environmental security, communications and operations management, access control, systems acquisition, development and maintenance, security incident management, business continuity management and compliance.
- The lottery has a robust physical and environmental security security control environement that includes; employee, vendor and visitor background checks, standard survellience monitoring and entry controls for all lottery facilities.

CSL Security Process Opportunities for Improvement

During the assessment of CSL’s information security controls for Information Technology systems and gaming operation processes, the following high risk areas for improvement were identified:

- IT disaster recovery plans (DRP).
- Consolidation and protection of system logs and monitoring administrator and operator activities.
- Assessment of system vulnerabilities.
- Information leakage.
- System test data protection.
- Ticket destruction, balancing and yearly inspections process.
- Information security risk assessment methodology.

BACKGROUND AND PURPOSE

The California State Lottery (CSL) was created by a 1984 ballot initiative that was approved by 58% of the voters. The portion of the initiative known as the California State Lottery Act of 1984, establishes the CSL as an independent state agency to market and sell lottery products to the California public.

In April 2010, the Legislature passed Assembly Bill 142, which changed the Lottery's funding formula to follow best practices. AB 142 limits administrative expenses to 13 percent of sales, while requiring that 87 percent of sales go back to the public in the form of prizes and contributions to education. AB 142 did not modify the mandated security review requirements noted in section 8880.46. The Act specifies that the CSL is operated and administered by a Commission appointed by the Governor. A Director, who is also appointed by the Governor, serves as executive officer for the CSL and manages all operations of the CSL.

The California State Lottery Act of 1984 requires the Commission to engage an independent firm experienced in security procedures, including but not limited to computer security and systems security, to conduct a comprehensive review and evaluation of key aspects of security in the operation of the CSL. The security audit will follow-up on past concerns noted in 2010 in addition to the requirements mandated by the Lottery Act of 1984 section 8880.46.

The CSL currently employs approximately 644 employees state-wide and has nine (9) district offices. There are also two (2) warehouses; one located in West Sacramento and one in Rancho Cucamonga. Corporate headquarters is comprised of eight (8) divisions and numerous subdivisions known as units.

CSL games are printed and shipped to the warehouses for delivery to retailers. Games are sold through retailers who have applied for and been approved to act in that capacity. Relationships between the CSL and its retailers are governed by CSL regulations as well as the agreement executed with each retailer.

The CSL retailer network consists of approximately 21,197 locations within supermarkets, drug stores, liquor stores, convenience stores, mall kiosks, markets (1-4 check stands) and various social settings. In addition to selling draw games through clerk operated terminals, the network includes 1,355 self-service consumer operated terminals.

Presently, most of the retailer network equipment communicates with the central gaming system through use of satellite or radio communication technology. Additional equipment used throughout the network includes approximately 4,014 instant ticket vending machines, 19,150 check-a-ticket devices used by players to verify whether a ticket is a winning one, and 4,622 video monitors used mainly for viewing Hot Spot game draws.

Retailers are equipped with a terminal provided by the CSL's gaming system vendor, GTECH Corporation, who issues tickets for the draw games, validates prize claims for all games, and interacts with the gaming system both to record wagers and to keep record of all retailer lottery product sales, prize payments, and other fiscal transactions.

The overall purpose of this engagement was to conduct a comprehensive review of all aspects of lottery security in accordance with the Lottery Act of 1984, section 8880.46. The review assessed the security measures that support the integrity, honesty and fairness of the CSL's operations, computer security, and system security. The following represents the objectives of the security assessment:

- Conduct a comprehensive review of lottery security in accordance with the Lottery Act of 1984, section 8880.46.
- Assess the security measures which support the integrity, honesty and fairness of the California State Lottery's operations, computer security, and system security.
- Promote continual improvement of CSL processes while assuring the public and player that CA games are secure and fair.

- Ensure that CSL has the right resources focused on the higher security risk areas.
- Ensure that the security policy framework and management processes mitigate the lottery's risk.

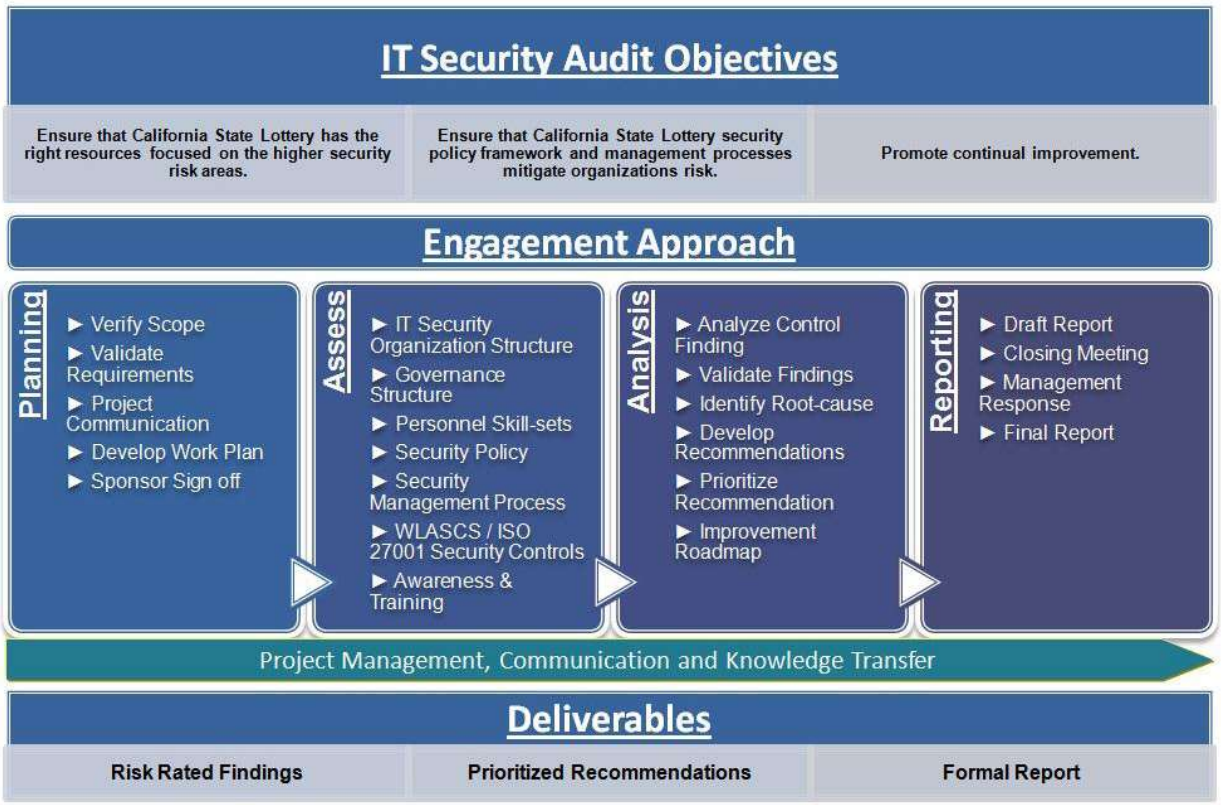
SCOPE OF SECURITY ASSESSMENT

As noted, the lottery is mandated by the Lottery Act of 1984 to complete a security review on a biennial basis. However, while the lottery is required to review the first 16 items noted below, it also recognizes that new and different security challenges have occurred since 1984. The lottery has not only engaged GLI to perform a security audit against the Lottery Act of 1984 section 8880.46, but in addition, the lottery has requested GLI hold the lottery to the highest gaming industry standard by including the internationally recognized standard from the World Lottery Association the Security Controls Standard (WLASCS: 2005) and the ISO 27001 Information Security Management standard (ISO 27001:2008). Areas of coverage include section 8880.46 as outlined below.

1. Personnel Security
2. Lottery Game Retailer security
3. Lottery Contractors security
4. Security of manufacturing operations of Lottery Contractors
5. Security against ticket counterfeiting and alterations and other means of fraudulently winning
6. Security of drawings
7. Computer security
8. Data communications security
9. Data base security
10. Security controls and physical security
11. Security in distribution
12. Security involving validation and payment procedures
13. Security involving unclaimed prizes
14. Security aspects applicable to each particular Lottery Game
15. Security against locating winners in Lottery Games having preprinted winners
16. Any other aspects of security applicable to the Lottery and its operations
17. Vulnerability assessment of CSL network devices, computer systems and website

APPROACH

The following audit approach was developed to fulfil the requirements as outlined within the Lottery Act of 1984 section 8880.46. GLI managed the section 8880.46 requirements listed above by grouping them logically and mapping them back to the various security control domains as described within industry best practice standards; World Lottery Association Security Control (WLASCS) and ISO 27001 Information Security Management (ISO 27001). This grouping facilitated an efficient and effective audit engagement. Our team utilized a standard risk based audit methodology for this engagement. Our audit process contained four phases: planning, assessment, analysis and reporting that delivers an effective, efficient and quality product.



APPLICABLE STANDARDS

Standard	Focus
Lottery Act of 1984, section 8880.46	1. Personnel Security 2. Lottery Game Retailer security 3. Lottery Contractors security 4. Security of manufacturing operations of Lottery Contractors 5. Security against ticket counterfeiting and alterations and other means of fraudulently winning 6. Security of drawings 7. Computer security 8. Data communications security 9. Data base security 10. Security controls and physical security 11. Security in distribution 12. Security involving validation and payment procedures 13. Security involving unclaimed prizes 14. Security aspects applicable to each particular Lottery Game 15. Security against locating winners in Lottery Games having preprinted winners 16. Any other aspects of security applicable to the Lottery and its operations
World Lottery Association: Security Controls Standard (WLA:SCS2006)	The WLA Security Control Standard (WLA-SCS) is designed to help Lottery and Gaming Organizers around the world achieve levels of

	control that are in accordance with both generally accepted information security and quality practices as well as specific industry requirements. WLA Security Control Standard© (WLA-SCS), the lottery sector's only internationally recognized security standard.
ISO/IEC 27001:2005 Information Security Management Standard	ISO/IEC 27001, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard (more below).

METHODOLOGY

GLI utilized the following methodology to conduct the security assessment against the CSL operations.

1. Planning
    a. Develop audit plan,
    b. Develop working papers, and
    c. Plan fieldwork audit based on risk.

2. Assess
    a. Perform document review,
    b. Identify lottery processes and interview processes owners,
    c. Identify and assess critical lottery systems, and
    d. Identify and scan network devices.

3. Analysis
    a. Complete analysis of findings, and
    b. Develop recommendations for improvement.

4. Reporting
    a. Develop draft report,
    b. Collect Management Response from CSL, and
    c. Complete final report.

Technical Assessment Approach

To fulfil the requirements of the audit with regard to other aspects of security applicable to the Lottery and its operation, along with a technical vulnerability assessment of CSL's network devices, computer systems and websit GLI utilized the following technical assessment approaches.

Wide-Area Network Testing (WAN)
Wide Area Network or (WAN) tests were designed with the goal of verifying that communication and data transfers between different geographic locations were configured and operated securely. This included reviewing configurations of routers and firewalls that may have a way (potential or actual) of communicating with anything outside of the local network.

- Compared diagrams provided to physical equipment to ensure proper setup.
- Reviewed and tested all configurations for hardware related to inter-location communication and verified traffic was properly routed and managed.
- Assessed and tested WAN monitoring software that was being used with a focus on any unrestricted access the software may have.
- Identified means and methods of enabling redundant ways of accessing important data and locations.

Local-Area Network Testing (LAN)
Local Area Network or (LAN) testing was designed with the goal of determining the security and redundancy of the CSL network. This included verifying all equipment was properly configured to protect the data passing through as well as ensuring there was a secondary method of running the network in the event a problem occurs. During the assessment the following activities were performed:

- Comparison of network diagrams provided to physical equipment to ensure proper setup.
- Identification of network connections to ensure redundancy within the LAN environment in both a physical aspect and a routing aspect.
- Reviewed and tested all configurations for hardware responsible for LAN traffic.
- Performed a threat analysis on critical systems using TCP and UDP endpoint tracing software and identified any traffic that could be a threat.
- Identified any network accessible file shares or other network storage areas that should be restricted.

System Testing
System testing was designed to analyze the servers and computers that were connected to the LAN which may have had an impact on the network. These tests were designed to look for security measures to protect other systems on the network and close any means of attacking the system through exploits. During the assessment the following activities were performed:

- Reviewed user account procedures in place for password management, access level security.
- Verified means to monitor account usage.
- Reviewed policies and procedures in place.
- Reviewed servers and workstations for security patches, virus scanning software and assessed the policies in place for updating both.
- Checked for any services that may have been running on high-ports or other uncommonly used ports.

Wireless Testing
Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that an organization assess risks more frequently as well as test and evaluate system security controls when wireless technologies are deployed.

- Identified wireless access points connected to the network and tested for best practice methods of securing wireless traffic.
- Reviewed and tested what algorithm is being used for password encryption on the access points, in addition to testing how servers/workstations utilize the access point.
- Attempted to brute force a connection to any wireless access points and attempt to gather data.

Port Scanning

The design and operation of the Internet is based on the Internet Protocol Suite more commonly referred to as TCP/IP. Hosts and services are referenced using an IP address and a port number ranging from 1 to 65536. Port Scanning tests are designed to verify that running systems and services are using proper ports and that unused ports are not being utilized for malicious intent.

- Performed a network scan of all open ports using Nessus Port Scanner and other related tools to review the results for open threats.
- Compiled a list of threats by general risk level from mild to severe.
- Checked for server-level and application-level logs and errors that may contain sensitive information.

SECTION TWO – ASSESSMENT RESULTS

The following section contains the results of the security assessment. This section has been divided to match the sixteen sections defined by the scope that is in compliance with section 8880.46 of the Lottery Act. We have provided a description of the controls reviewed in each section along with the identified areas that GLI has provided high-level recommendations for continual improvement.

COMPUTER SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: Information security policy, security organization, asset management, information classification, information security incident management, business continuity management, and compliance.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- IT disaster recovery plans (DRP)

DATA COMMUNICATION SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: IT operations procedures, third-party management, system planning, testing and acceptance, protection against malicious code, data back-up, network security controls, media handling, secure exchange of information, electronic commerce, network monitoring and cryptographic controls.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- Consolidation and protection of system logs and monitoring administrator and operator activities
- Assessment of system vulnerabilities

DATABASE SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: user access control, network access control, application access control, mobile computing, system security requirements, and system control of data, cryptographic controls, and security of system files, end user support processes, remotes access management and technical vulnerability management.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- Information leakage
- System test data protection

SECURITY CONTROL AND PHYSICAL SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: physically secure areas, equipment security, and environmental controls for the protection of network resources.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No high risk findings or recommendations were noted within the audit area

PERSONNEL SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: employee background check, human resource policy, process for integration of new employees and the termination of employee and security awareness and training.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No high risk findings or recommendations were noted within the audit area

LOTTERY GAME RETAILER SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: retailer recruitement and set-up, retailer operations, gaming terminal security, and retailer security of instant tickets.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No high risk findings or recommendations were noted within the audit area

CONTRACTOR SECURITY (THIRD PARTY / VENDOR)

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes: GTECH gaming operations process, firewall management, vulnerability management process, data center security, system change management, and systems operation procedures.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

MANUFACTURING OPERATIONS SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include: instant game design, gaming terminal security and instant game closure.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- Ticket destruction, balancing and yearly inspections process

SECURITY AGAINST TICKET COUNTERFEITING, ALTERATIONS, AND FRAUDULENT WINNING

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes instant ticket printing.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

SECURITY IN DRAWINGS

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include; lottery draw management, conducting a draw and management of physical draw appliances and ball sets.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

SECURITY IN DISTRIBUTION

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas

reviewed as a part of Computer Security include; shipment of instant tickets and storage and distribution of instant tickets.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No high risk findings or recommendations were noted within the audit area

VALIDATION AND PAYMENT SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes prize protection and validation processes.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

UNCLAIMED PRIZES SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes unclaimed prize money protection processes.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

PARTICULAR GAME SECURITY

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security include; instant "scratcher" tickets and game draws.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

SECURITY AGAINST LOCATING WINNERS FOR GAMES HAVING PREPRINTED WINNERS

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes; protection of validation numbers and winner files and instant ticket control system.

Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- No findings or recommendations were noted within the audit area

OTHER ASPECTS OF SECURITY APPLICABLE TO THE LOTTERY AND ITS OPERATIONS

GLI's assessment of the Computer Security processes included, inquiry into the controls and administrative practices that are both internal and external to the reporting structure of the CSL. Areas reviewed as a part of Computer Security includes; information security management system processes and security organization structure. Also included in this assessment area was a vulnerability assessment of the CSL corporate local area network, wireless network access controls, and scan of the public website.
Based on the security assessment, GLI has provided recommendations deemed to be of a high risk to the organization covering the following areas:

- Information security risk assessment methodology

CONCLUSION

GLI completed the evaluation of California State Lottery network on 19 February 2013.

Subject to the limitations discussed in this report it is GLI's position that the evaluated elements of California State Lottery network and gaming operation comply with the applicable sections of the standards listed herein. Subject to these limitations, GLI determines that the California State Lottery in compliant to the Lottery Act of 1984 section 8880.46.

TERMS AND CONDITIONS

GLI's audit conclusions for the security assessment of the California State Lottery (CSL) are conditional upon the following:

- The evaluation of CSL's network and gaming operation was related to the documented scope only. This excludes any other functions,
- The information gathered from CSL personnel is assumed to be accurate and complete,
- The Internet-facing systems tested were limited to the address ranges provided by CSL,
- Network conditions are ideal, and the tools used to perform the testing are assumed to operate as intended and bug-free,
- Legal Compliance with requirements is outside of the scope of GLI's evaluation, and
- There are unavoidable limitations inherent to performing an audit within a short period of time, as it is not possible to verify the effects of all of potential configurations and environments that may occur once the site is running in the production for an extended period of time.

Authentication of Gaming Laboratories International, LLC's Final Report for the security assessment of the California State Lottery.

Signed: _____ Date: 2-19-13

CSL EXECUTIVE RESPONSE

February 13, 2013

Gregory Doucette, Director
Global Professional Services
GLI Test Labs Canada
Suite 104 - 910 Main Street
Moncton, NB, Canada, E1C 1G6

Subject: Biennial Security Audit 2012

Dear Mr. Doucette:

The foundation of the California State Lottery (Lottery) is built on integrity and fairness in its games. As such the Lottery is committed to incorporating industry leading practices identified throughout this audit including World Lottery Association Standards. Thank you for your comprehensive and thorough assessment that will contribute to improvements in our processes and practices.

The 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 leading practices that Lottery can embrace to assure the public and players that Lottery games are secure and fair.

Sincerely,

Robert T. O'Neill
Director