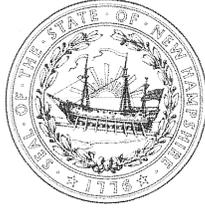


**STATE OF NEW HAMPSHIRE  
LOTTERY COMMISSION**

**MANAGEMENT LETTER  
FOR THE FISCAL YEAR ENDED JUNE 30, 2011**



JEFFRY A. PATTISON  
Legislative Budget Assistant  
(603) 271-3161

MICHAEL W. KANE, MPA  
Deputy Legislative Budget Assistant  
(603) 271-3161

## State of New Hampshire

OFFICE OF LEGISLATIVE BUDGET ASSISTANT  
State House, Room 102  
Concord, New Hampshire 03301

RICHARD J. MAHONEY, CPA  
Director, Audit Division  
(603) 271-2785

*To The Fiscal Committee Of The General Court:*

We have audited the financial statements of the New Hampshire Lottery Commission (Lottery), a department of the State of New Hampshire, as of and for the fiscal year ended June 30, 2011 and have issued our report thereon dated December 21, 2011.

This management letter, a byproduct of the audit of the New Hampshire Lottery Commission for the fiscal year ended June 30, 2011, contains our auditor's report on internal control over financial reporting and on compliance and other matters and related audit findings. The appendix, included as an attachment to the management letter, provides a summary of the status of observations presented in the fiscal year 2010 management letter of the Lottery Commission.

The Lottery is again submitting its comprehensive annual financial report (CAFR) to the Government Finance Officers Association (GFOA) for consideration for the GFOA's Certificate of Achievement for Excellence in Financial Reporting. A certificate of achievement is a prestigious national award for CAFRs that are prepared in accordance with program standards. The program standards are intended to promote easily readable and understandable financial reports that demonstrate financial accountability and comparability. The Lottery received GFOA certification for its 2010 CAFR, and it is believed that the 2011 CAFR also conforms to the certificate of achievement program requirements. A copy of the Lottery's 2011 CAFR can be obtained from the New Hampshire Lottery Commission, 14 Integra Drive, Concord, NH 03301. The Lottery CAFR can also be accessed online at:

[http://www.gencourt.state.nh.us/LBA/AuditReports/FinancialReports/pdf/Lottery\\_2011\\_CAFR.pdf](http://www.gencourt.state.nh.us/LBA/AuditReports/FinancialReports/pdf/Lottery_2011_CAFR.pdf).

*Office of Legislative Budget Assistant*  
Office Of Legislative Budget Assistant

December 21, 2011

STATE OF NEW HAMPSHIRE  
LOTTERY COMMISSION  
2011 MANAGEMENT LETTER

TABLE OF CONTENTS

	<u>PAGE</u>
Letter Of Transmittal.....	i
<b>Auditor’s Report On Internal Control Over Financial Reporting And On Compliance And Other Matters *</b> .....	1
<i>Internal Control Comments</i>	
<i>Significant Deficiencies</i>	
1. Controls Over Game Draws Should Be Improved .....	3
2. Controls Over Preparation Of Financial Statements Should Be Improved .....	4
3. Compliance With Financial Control Activities Should Be Improved .....	6
4. Policies And Procedures For Posting Ticket Cost Data Should Be Established .....	7
5. Risk Assessment Should Be Performed.....	7
6. Controls Over Replay Program Should Be Improved .....	9
7. Segregation Of Duties Should Be Improved Over Merchandise Prizes- Replay Program .....	12
8. Controls Over Keycards Should Be Improved .....	13
9. Vendor Compliance With Insurance Requirements Should Be Monitored And Enforced .....	15
<i>State Compliance Comment</i>	
10. Prize Claims Should Be In Compliance With Rules .....	17
<i>Review Of Lottery Information Technology System General Controls</i> .....	19
<b>APPENDIX - Current Status Of Prior Audit Findings</b> .....	35

\* No audit comments suggest legislative action may be required.

This report can be accessed in its entirety on-line at:  
<http://www.gencourt.state.nh.us/LBA/AuditReports/financialreports.aspx>



JEFFRY A. PATTISON  
Legislative Budget Assistant  
(603) 271-3161

MICHAEL W. KANE, MPA  
Deputy Legislative Budget Assistant  
(603) 271-3161

**State of New Hampshire**  
OFFICE OF LEGISLATIVE BUDGET ASSISTANT  
State House, Room 102  
Concord, New Hampshire 03301

RICHARD J. MAHONEY, CPA  
Director, Audit Division  
(603) 271-2785

## **Auditor's Report On Internal Control Over Financial Reporting And On Compliance And Other Matters**

*To The Fiscal Committee Of The General Court:*

We have audited the financial statements of the New Hampshire Lottery Commission as of and for the fiscal year ended June 30, 2011 and have issued our report thereon dated December 21, 2011. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

### Internal Control Over Financial Reporting

In planning and performing our audit, we considered the Lottery Commission's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Lottery Commission's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Lottery Commission's internal control over financial reporting.

*A deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of the internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting described in Observations No. 1 through No. 9 as well as the information technology observations listed on page 19 under the headings of General Comments, Governance, and Access to Programs and Data to be significant deficiencies

in internal control over financial reporting. A *significant deficiency* is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

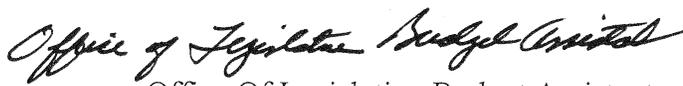
The observations listed on page 19 under the heading of Process Improvement Opportunities are not considered significant deficiencies but are reported for management's information.

#### Compliance And Other Matters

As part of obtaining reasonable assurance about whether the Lottery Commission's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, rules, regulations, and contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*. However, we noted one instance of immaterial noncompliance which is described in Observation No. 10.

The Lottery Commission's written responses to the observations in this report have not been subject to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the management of the New Hampshire Lottery Commission, others within the Lottery Commission, and the Fiscal Committee of the General Court, and is not intended to be used by anyone other than these specified parties.

  
Office Of Legislative Budget Assistant

December 21, 2011

**Internal Control Comments**  
**Significant Deficiencies**

**Observation No. 1: Controls Over Game Draws Should Be Improved**

*Observation:*

A review of Lottery Commission (Lottery) draw practices indicates that Lottery should consider tightening controls over that critical activity.

Lottery performs regular drawings for both New Hampshire Lottery and Tri-State Lottery games. Manual drawings are performed using game machines that employ numbered balls and devices to randomly select numbered balls to determine winning numbers. The game balls and machines are contained in a secured room at Lottery headquarters. Policies and procedures for the drawings provide for test draws to check for mechanical functioning and apparent randomness of ball selection, video taping, and observation of the actual draws by a representative of a contracted certified public accountant (CPA).

1. In reviewing the videos of a sample of 10 drawings that occurred during fiscal year 2011, we noted four instances where one or more of the game balls used in the drawing were dropped during the test draw process. When this occurred, the balls were simply picked up off the floor and the test draw continued. The mishandling of the game balls often appeared to be the result of the draw individuals not taking due care with the draw process. In the instances noted, neither Lottery's employees performing and recording the draw nor the contracted CPA representative observing the draw expressed concern that the game balls were mishandled.
2. The Lottery experienced a critical game draw problem in August 2011. The Lottery reported the employee who performed a game draw subsequently realized that a critical error had occurred in the prior evening's draw. Lottery's review of the draw tape revealed the draw machine had not been completely cleared from the results of a test draw prior to the official game draw. Neither the employee performing the draw duties, the videographer, nor the contracted observer noted that a ball selected in a test drawing remained as a selected ball in the actual game drawing. Once the error was recognized, Lottery performed a second drawing a day after the initial drawing. Approximately \$4,500 of additional prizes were awarded as a result of the extra drawing.
3. Effective May 1, 2011, Lottery established a revised Tri-State Winning Number Draw Policies and Procedure Manual (Manual) which included policies and procedures to better control access to the draw room and equipment in the room. While certain weaknesses noted in the prior management letter were addressed by the new policies and procedures, a review of the draw room access logs for the months of May and June 2011, indicated not all entries to the draw room occurring outside of normal draw times were appropriately supported by advanced written notification, as specified in the Manual. Additionally, a review of the written notifications supporting access recorded in the logs indicated the draw room was

accessed outside of non-draw times for reasons other than those allowed by the Manual, and advanced notice was not always provided prior to employees accessing the draw room.

4. While Lottery's Security Director receives the notifications of the intended draw room access, the Security Director's designee for this responsibility is the employee primarily responsible for the conduct of the draws, creating a segregation of duties weakness. The employee responsible for monitoring access to the draw room should not also have regular access to that secured room.

*Recommendation:*

Lottery should improve the controls and exhibit increased due care in the performance of all game draw activities, including test draws, security over the game draw equipment, monitoring access to the draw room, and the actual performance of the game draws.

Lottery should monitor its game draw control activities to ensure policies and procedures for draw security are adhered to and enforced. The responsibilities of the Lottery Security Officer, including designee, should be appropriately segregated from other Lottery game draw responsibilities.

*Auditee Response:*

We concur. The Lottery will investigate and consider solutions for this observation in accordance with the statutory requirements as provided by the Tri-State Compact and in particular, RSA 287-F:5, V and RSA 287-F:5, VIII - Governing Procedures and Conditions.

**Observation No. 2: Controls Over Preparation Of Financial Statements Should Be Improved**

*Observation:*

Errors noted in Lottery's preparation of its statement of cash flows for fiscal year 2011 indicate a weakness in Lottery's process for accumulating and summarizing data reported by that statement.

The Lottery used numerous spreadsheets and State accounting system (NHFirst) reports to identify and accumulate amounts to be reported on its fiscal year 2011 statement of cash flows. Our review of the statement of cash flows and documentation supporting the statement noted the following financial reporting errors related to payments made to Lottery's joint ventures:

- \$493,000 understatement of cash outflows resulted from an undetected spreadsheet calculation error.
- \$584,000 understatement of cash outflows resulted from the misposting of two amounts on a supporting spreadsheet.

- \$208,000 understatement of cash outflows resulted from an error in criteria used to draw account data from NHFirst.

The above noted errors also resulted in a \$1,285,000 offsetting overstatement of cash outflows from payments to suppliers for goods and services.

Although the Lottery has experienced ongoing problems in reviewing its cash transactions recorded in NHFirst and those continuing problems may have contributed to Lottery's difficulties in preparing an accurate statement of cash flows for inclusion in its comprehensive annual financial report for June 30, 2011, each of the above noted errors should have been detected by the Lottery if a reasonable review of the supporting documentation had occurred when the statement was prepared.

*Recommendation:*

The Lottery should review its process for preparing its financial statements to ensure the process provides reasonable review and approval controls to promote accurate financial reporting, including preparation of the statement of cash flows. The Lottery should also ensure employees involved in financial reporting are appropriately trained in their respective duties and arrange for additional training, as required.

*Auditee Response:*

We concur. The Lottery has met with the Department of Administrative Services on this matter. The NHFirst system (Lawson) cannot separately report Lottery's cash activity from that of the State's Racing and Charitable Gaming Commission (RCGC), also accounted for in the State's Sweepstakes Fund cash account. In order to compensate for this control weakness in Lawson, the Lottery has to dedicate a great deal of resources to manually re-create a separate sub-system for cash payments. This sub-system does not resolve the issue, but merely helps Lottery create a "reasonable" cash amount that represents Lottery-only cash activity (without RCGC). Unfortunately, the Lottery needs cash to be separated in order to produce financial statements. This weakness in Lawson makes it impossible to reconcile to an exact dollar amount; however using this sub-system allows us to come within a non-material difference.

The Lottery agrees that there was a misclassification of three payments in the manual sub-system, outside of Lawson. In total, cash payments were not misstated; however the classification/title of the payments used was mislabeled in the sub-system. The Lottery was able to correct the misclassification on the cash flow statement.

The Department of Administrative Services has advised Lottery that they are seeking a resolution to separate Lottery cash activity from RCGC cash activity in the Lawson accounting system. The Lottery will continue to work with the Department of Administrative Services to address this risk.

### **Observation No. 3: Compliance With Financial Control Activities Should Be Improved**

#### *Observation:*

An instance was noted where one of Lottery's primary financial controls did not operate as expected during fiscal year 2011. The failure of this control raises concerns as to the control consciousness of Lottery employees and whether employees are fully aware of the importance of consistent and accurate performance of control activities.

It is a Lottery claims-payment control, established through policy and procedure, that all prize claims exceeding \$599 receive management approval and all prize claims greater than \$5,000 receive additional supervisory approval, prior to payment. The performance of the control is evidenced by a responsible party initialing the claim form to document a review and approval for the payment. During testing of claims payments, we noted one paid jackpot claim totaling \$804,218 which lacked evidence of management's review and approval. This claim was one of three jackpot prizes paid by the Lottery during fiscal year 2011.

The processing of a significant prize payment without the required evidence that the requisite approval had been applied is a significant control failure that increases risk that erroneous or fraudulent payments could be made without detection and correction.

A similar comment was included in the fiscal year 2010 management letter.

#### *Recommendation:*

The Lottery should improve compliance with its control activities. Employees should be adequately trained in the control activities and the importance of consistent performance of those control activities. The Lottery should ensure employees are aware of the control purpose and proper control procedures. Employees should be reminded that they should not allow further processing of a transaction if required reviews and approvals are not evident.

#### *Auditee Response:*

We concur. This prize payment was paid by the Tri-State Lotto office located at Vermont Lottery. When a Tri-State jackpot winner visits the New Hampshire Lottery for payment, a member of management works with the winner in gathering all the necessary documentation required to process payment. Tri-State requires that a member of management forward them proper documentation and follow established procedures before payment can be made. In this particular case, the Marketing Manager sent a signed written letter and a signed qualified prize option advisory form to the Tri-State office requesting payment directly to the winner. Security initialed and verified the validity of the prize and ran required system reports. All of this documentation was in the winners file.

The Marketing Manager did not initial the claim form itself, but the Security Director initialed the claim form. The file had a signed written letter and a prize advisory form signed by management, proving the prize was approved for payment.

**Observation No. 4: Policies And Procedures For Posting Ticket Cost Data Should Be Established**

*Observation:*

The Lottery has not established policies and procedures for a review of instant ticket cost information posted to the Lottery's gaming system (the Back Office System, or BOS). The lack of policies and procedures contributed to the condition that during two months of fiscal year 2011 no review of the input of this information occurred.

During the first eleven months of fiscal year 2011, ticket cost information was entered into the BOS without a formal review and approval control. While an informal review was performed, this control activity ended part way through the year upon the retirement of the employee who performed the review. The review process began again in late June in preparation for the yearly physical inventory of tickets on hand. Even when the review was performed, it was never sufficiently evidenced to allow it to be considered an effective control activity. Lottery reported on July 13, 2011 that it will check costs for new games monthly as they go on to the market for sale.

*Recommendation:*

The Lottery should establish policies and procedures for reviewing and approving instant ticket cost data entered into BOS, similar to policies and procedures for reviewing and approving other accounting entries.

Ticket cost information should be entered into BOS and reviewed when the ticket inventory is received.

*Auditee Response:*

We concur. As of December 2011 new procedures were established to ensure ticket costs are accounted for correctly. Part of these procedures include the General Ledger Accountant receiving copies of all receiving slips and verifying they are entered into the gaming system correctly.

**Observation No. 5: Risk Assessment Should Be Performed**

*Observation:*

The Lottery performed only one of its semiannual risk assessments during fiscal year 2011. As of November 23, 2011, the Lottery had not taken specific actions in response to risks identified as a result of its May 2011 risk assessment.

A primary tenet of effective internal controls is an organization's periodic assessment of and reaction to the risks it faces. Without this proactive approach to risk, an entity operates in a reactive mode, often addressing risks only after a loss has been incurred.

During fiscal year 2011, the Lottery implemented a new gaming system serviced by a new vendor. The gaming system is the computerized platform used to process essentially all Lottery ticket sales, validate all winning tickets, and control inventory of tickets. The change in the Lottery's gaming system came at a time when Lottery reportedly no longer had experienced and embedded Department of Information Technology (DoIT) support personnel. While the lack of experienced and embedded information technology (IT) support was identified as a serious concern by Lottery's Chief Security Officer and Executive Director, no formal reassessment of Lottery's IT needs was performed during fiscal year 2011. In fact, risk related to IT operations, specifically disaster recovery, was identified as a primary risk in the May 2011 risk assessment. This risk was exemplified by some Lottery managers being apparently unaware of the existence of a Lottery Disaster Recovery Plan.

*Recommendation:*

The Lottery should adhere to its policies and procedures and perform at least semiannual risk assessments as provided for in the Lottery's policies and procedures manual. Action should be taken to mitigate identified risks.

As further discussed in the information technology observation III.D.1, Disaster Recovery and Business Continuity Plan on page 30, Lottery and Department of Information Technology management should document a plan to provide the information technology support needed to update and periodically test the Lottery's disaster recovery plan as soon as possible.

*Auditee Response:*

We concur and do understand the importance of this process. We are in the process of addressing the risk assessments.

*Department of Information Technology Response:*

We concur with the observation that a risk assessment should be performed. As part of the observation, it was noted that during the change of Lottery's gaming vendor, there was not an "experienced and embedded Department of Information Technology (DoIT) support personnel". And that "no formal reassessment of Lottery's IT needs was performed during fiscal year 2011." During fiscal year 2011, a new Agency Technology Manager (ATM) began work at Lottery. The new ATM is embedded half time at Lottery and began an assessment of Lottery's needs. Since that time, the support model for Lottery has changed at the desktop level and at the IT management level. More focus is being placed on the interoperability of State and gaming vendor devices and a plan is being undertaken to document all connections and interdependencies. It is anticipated that the plan will be ready for implementation by September 1, 2012.

Semiannual risk assessments: Currently, the Agency Technology Manager is not part of the management meetings. It would be beneficial to both Lottery and DoIT for the ATM to attend these meetings. Oftentimes, information presented and discussed in these meeting will have significant impact on interpretation of both risks and policies and procedures.

Disaster recovery and continuity of operations plans: Work has already begun on updating the disaster recovery (DR) Plan to align with the new vendor and to create a test plan going forward. A failover test is being planned for later in March 2012 to identify areas where the DR Plan needs to focus and as a partial DR test.

### **Observation No. 6: Controls Over Replay Program Should Be Improved**

#### *Observation:*

Unaddressed weaknesses in Lottery's controls over its Replay program increase the risks the Replay program will not operate as intended by Lottery management, exposing the Lottery to unanticipated financial risks and risk of loss of consumer confidence. While risks to Lottery's operations related to the lack of documentation of the operation of the Replay program was first noted in the 2009 audit management letter, the Lottery has not taken reasonable and timely action to improve its controls over the Replay program system since that initial observation, even while it has significantly expanded its use of the Replay system to select second-chance game winners for its instant ticket games, starting in fiscal year 2010 and continuing into fiscal year 2011.

The Lottery's Replay program is primarily an Internet-based second-chance game where players, upon registering and providing certain personal information, can enter non-winning Lottery tickets in exchange for Replay Points. These points can be used to purchase entries for drawings to win various merchandise prizes, which have been provided by businesses (advertising partners) in exchange for promotional consideration on the Replay website. The Lottery and its advertising vendor use the players' demographic information in marketing the Lottery's games. The Replay system is comprised of a website, database, and random number generator (RNG). Drawings are held monthly using the RNG to select winners from the population of entries.

As noted in the fiscal year 2010 audit management letter observation,

1. All three components of the Replay system, the website, database, and RNG, are operated and maintained by the Lottery's advertising vendor. The Replay website, including the related Lottery player information database, is hosted by the Multi-State Lottery Association (MUSL) data center. Neither the initial Replay program agreement between the Lottery and the vendor nor subsequent contracts addresses the responsibilities for error detection, security breaches, and processing disruptions.
2. The Lottery relies upon its advertising vendor for the security of the personal information, including names, e-mail and residential addresses, and dates of birth, collected from registering players. There are no documented policies, procedures, or other agreements

describing the rights and responsibilities for the use and security of that confidential information.

3. There are no documented policies and procedures to address risks related to vendor or advertising partner performance.
4. During fiscal year 2010, the Lottery began to use the Replay system to conduct second-chance drawings for certain instant ticket games. During fiscal year 2011, the Lottery used the normal monthly Replay drawings procedures and RNG algorithm to conduct 15 second-chance drawings for its instant games. Prizes for these drawings ranged from \$10,000 to \$250,000 and totaled \$1,075,000.

While the RNG algorithm used for the drawings was independently certified during the development of the Replay system in 2006, the Lottery has not performed tests and established controls to ensure the security of the algorithm and the entries included in the population of entries subject to selection by the algorithm. The Lottery relies on the advertising vendor's implied assurances that all player data and Replay drawing entries are obtained, recorded, and secured. As a result, the Lottery may not be aware if entries were inappropriately included or excluded from drawing populations.

During fiscal year 2011, a regular Lottery review of Replay entrants for a monthly drawing noted two entrants who were known employees of the advertising vendor. In response, Lottery postponed the drawing to the following day to allow the vendor the opportunity to remove the employee entries from the drawing. The vendor subsequently reported the employee entries were included as test data for system tests performed by the vendor employees and, presumably through oversight, the test items were not removed from the data at the completion of the tests.

As a result of this incident, Lottery requested the vendor implement new security policies and procedures. A review of those policies and procedures noted five out of six advertising vendor employees had full administrator access to the Replay system. Administrators have the access and ability to add/remove replay points and edit player account details, reportedly because these access levels were necessary to respond to customer service issues. It is highly unusual to give essentially all users this highest level of access to such a critical system.

*Recommendation:*

As noted in the fiscal year 2009 and 2010 management letters, the Lottery should ensure that all critical aspects of, and responsibilities for, the Replay program and system are fully understood and documented by current contracts, agreements, and system documentation.

The Lottery should require its advertising vendor to establish and document the controls provided in the Replay system to ensure the integrity of the Replay system to draw Lottery game prizes. Those documented controls should include information technology general and application controls including administrative and other access controls, program change controls, regular plans of system monitoring and testing, and reviews of the security over the Replay system and the information the system contains.

The Lottery should require its advertising vendor to provide a yearly report on controls at a service organization relevant to security, availability, processing integrity, confidentiality and privacy, commonly known as a SOC 2 report, prepared by a certified public accounting firm based on its review of the Replay program's internal controls.

*Auditee Response:*

We do not concur.

With regard to the numbered fiscal year 2010 comments repeated this year:

1. Though maintained by an agency partner, the New Hampshire Lottery Replay website and related database system is hosted in a highly secured web environment, behind a secure firewall service operated and managed by the Multi-State Lottery Association (MUSL).

Database system access is restricted from the outside-world, and only through the actual website/web server.

Regular website content updates are performed first in development, and staging environments prior to launch on live website to ensure accuracy of delivered updates/solution as well as to eliminate potential conflicts with 'live' site functionality and code.

Player-level game-play errors and activity are reported on a regular basis via email notifications to both New Hampshire Lottery staff (for both marketing and legal compliance staff) and marketing agency technical staff. We are currently working on a SmartPhone application that we believe will dramatically reduce user time and errors, for players that possess such a device.

Daily incremental and weekly full data back-ups are performed automatically, to allow for system restoration or review, in the event of user-specific or system-wide errors.

2. The New Hampshire Lottery Replay rules outline that all information supplied to New Hampshire Lottery via account creation is private and will not be shared.

Security methods of all player information are outlined above.

3. Agency partner maintains a separate development environment for creation of all new website enhancements and features.

The New Hampshire Lottery contract with MUSL includes a staging/review server entirely separate, but mirroring the live/production environment – this staging server is used for final review/approval and testing of new services and enhancements.

Final/approved changes to the Replay application or database environment is performed following system-wide back-ups, and with advance notice to players for the known periods of downtime.

4. As discussed in the response to Observation No. 10, the issue related to second-chance drawings is no longer applicable.

With regard to the current year comment regarding vendor employee access to the system:

It is at the New Hampshire Lottery's discretion to allow the advertising vendor staff access to all areas of the administrative tool controlling New Hampshire Lottery Replay.

Restrictions of this will only limit the ability of the New Hampshire Lottery to quickly and efficiently address customer/player concerns as the multiple agency administrators allow for redundancy in coverage and support in times of need.

*LBA Rejoinder:*

As indicated by this continuing comment, we do not agree that Lottery has adequately documented responsibility for the implementation and ongoing effectiveness of controls for its Replay program. While Lottery may conclude there is a distinct separation of responsibility between itself and its vendors for the secure operation of Replay, it is not clear that Lottery's customers would see that same distinction if errors, frauds, or abuse of the Replay program occurred or were perceived as having occurred. Such an event, whether the responsibility of Lottery or its Replay vendor, could dramatically impact the Lottery's goodwill with its customers.

#### **Observation No. 7: Segregation Of Duties Should Be Improved Over Merchandise Prizes – Replay Program**

*Observation:*

The design of the Lottery's controls over merchandise prizes used in the Lottery's Replay program does not provide for an adequate segregation of duties to reasonably ensure control activities are, and remain, effective. During fiscal year 2011, the Lottery reported it awarded \$289,056 in Replay merchandise prizes. At June 30, 2011, the Lottery reported \$67,160 of Replay merchandise prize inventory on hand.

Efforts taken by the Lottery in fiscal year 2011, in part in response to a fiscal year 2009 audit comment, improved but did not resolve segregation of duties concerns over Replay program merchandise prizes.

In response to the fiscal year 2009 comment, the Lottery implemented several procedures which improved controls but did not fully mitigate the segregation of duties issue, as a lack of independent review for appropriate distribution of prizes continues. One employee continues to be responsible for the conflicting responsibilities of maintaining custody of prize merchandise, distributing the prizes, and maintaining the prize inventory record. Although a year-end inventory of contributed prizes is completed by tracing and agreeing the inventory on hand

according to the record of prizes on hand, the inventory procedure would not detect errors or frauds perpetrated by the custodian of the records and the merchandise.

The lack of segregation of duties in the Lottery's controls over the receipt, holding, disbursement, and reporting of Replay program merchandise prizes increases the risk that errors or frauds may occur in the merchandise prizes that would not be detected and corrected in the normal course of business.

*Recommendation:*

The Lottery should establish effective segregation of duties over accepting, holding, reporting, and disbursing merchandise prizes for its Replay program. Inventory activity and records should be periodically reviewed and compared to ensure that the inventory is properly controlled and reported.

*Auditee Response:*

We do not concur. When a prize arrives, a Clerk III or Laborer counts and records the number received. An email is sent to the Product Marketing Manager as to the name of the partner and the count. That employee then gives the prize to the Marketing Coordinator to count. The Marketing Coordinator counts and records the number received and adds the information to the Replay Prize spreadsheet. The number received is compared to the signed contract received. The Product Marketing Manager compares the two separate reports and initials the review. If there is a discrepancy, either party does a re-count. At the end of the Fiscal Year, an Accounting Technician does a complete inventory on hand. That review, done independently, is compared to the Replay Prize Spreadsheet.

*LBA Rejoinder:*

The risk expressed in the observation relates to the broad scope of control over Replay prizes exercised by one Lottery employee. Lottery's described process does not mitigate the risk resulting from one employee having responsibility for the incompatible functions described in the observation.

**Observation No. 8: Controls Over Keycards Should Be Improved**

*Observation:*

Lottery security personnel did not fully control certain unused keycards during fiscal year 2011. Keycards are used to regulate entry to restricted areas of the Lottery building. While unused keycards were reportedly physically secured, the access authorities on the unused keycards were not consistently deactivated in a timely manner.

The Lottery limits and monitors access to secure areas within the Lottery building in part through the use of computerized door locks. To gain entry to a restricted area, an employee with access

authority swipes an assigned security card across a keycard reader and enters a numeric personal identification number (PIN code) into a keypad. If the card and the PIN code match, the door unlocks. If the card and PIN code do not match, the door does not unlock. The keycard lock system includes an audit trail and other security features.

During a review of the system, we noted several active cards that were not currently assigned or were assigned to former employees. Five employees were assigned more than one card, one card was assigned to an employee of the Lottery's gaming system vendor, and one card provided to an auditor to use during the audit was not identified as having been assigned and did not have a recorded PIN code, even though the card was in use and necessarily had an associated PIN code.

According to the Lottery, the noted unassigned cards were either in the possession of the Lottery's Security Director or did not have recorded PIN codes in the system; either condition would prevent the cards from being misused.

*Recommendation:*

The Lottery should limit its exposure from the potential misuse of keycards by electronically securing or deactivating unused cards in a timely manner. All keycards in use should be formally assigned to individuals. Unnecessary duplicate cards should be collected and deactivated.

The Lottery should review the condition that allowed the auditor to use a keycard without a PIN code being reported by the system to determine whether there is an unrecognized weakness in the system's reporting.

*Auditee Response:*

We concur. The Lottery does supervise the issuance of keycards to non-agency personnel including the gaming vendor, DoIT, and auditors with the Office of Legislative Budget Assistant. Given the nature of the long term duties and responsibilities that require uninterrupted access to the site, the issuance of keycards in these circumstances is deemed appropriate by the Lottery. Similarly, Lottery employees are issued access keycards by the on-line gaming vendor and other business partners, for access to their facilities.

With regard to the condition observed by the auditor; the circumstances were reviewed in a timely manner following the auditor's control test. The review determined that the system did function correctly in that it denied access to the testing auditor while simultaneously alerting Lottery Security via an electronic alarm signal. Additionally, the auditor's image was recorded by motion activated surveillance cameras during all phases of the control test.

As recommended, the Lottery has improved upon our efforts to secure and deactivate unused cards in a timelier manner.

## **Observation No. 9: Vendor Compliance With Insurance Requirements Should Be Monitored And Enforced**

### *Observation:*

During fiscal year 2011, the Lottery did not require vendors to maintain current insurance certificates on file, even though Lottery's contracts require certain prime vendors to provide that proof of relevant insurance coverage to the Lottery.

A review of insurance certificates on file at Lottery during fiscal year 2011 noted vendors did not consistently provide the Lottery with evidence of renewed coverage for a number of certificates which expired during the fiscal year.

#### 1. Gaming System Vendor

The certificates of insurance coverage for workers compensation and property insurance expired in November 2010. There was a lapse in insurance coverage against Errors and Omissions between May 30, 2011 and June 27, 2011. Fidelity bond coverage did not become effective until November 1, 2010, four months after the effective date of the contract. There was no certificate on file to support property insurance coverage for the vendor's Vermont data center, which is a critical hub of the Lottery's Gaming System.

At the time of the auditor's inquiry, the Lottery was apparently unaware that current certificates had not been furnished by the vendor. Subsequent to the auditor's inquiry, the Lottery obtained certificates of insurance coverage for workers compensation and property insurance.

#### 2. Instant Ticket Vendor

The certificate of insurance coverage on file for general liability insurance expired on October 31, 2010. The Lottery did not have a subsequent certificate of insurance coverage on file. There also was no evidence on file that a fidelity bond required by the contract was in effect during the audit period.

#### 3. Advertising Vendor

The certificate of insurance coverage on file for General Liability insurance expired on January 1, 2011. The Lottery did not have a subsequent certificate of insurance coverage on file.

The Lottery reported that miscommunication regarding the assignment of responsibility for monitoring vendor compliance with insurance requirements contributed to Lottery's ineffective monitoring of vendor compliance with those contractual insurance requirements.

The lack of appropriate insurance coverage in place for prime vendors could seriously impact the Lottery's ability to rely upon the continued performance of those vendors if a calamity struck the vendor's operations.

*Recommendation:*

The Lottery should require vendors to comply with all contract provisions. The Lottery should actively monitor vendor compliance with all significant contract provisions, including requirements for vendors to prove maintenance of required insurance coverage.

The Lottery should ensure that it has clearly assigned and communicated to responsible employees the duty to monitor vendor compliance with significant contract provisions intended to protect the interests of the Lottery, including evidencing required insurance coverage. Employees should notify senior Lottery management immediately if prime vendors fail to maintain contractually required insurance coverage.

*Auditee Response:*

We concur. We now have a central file of all insurance certificate documents for all contracts and a database reminder process.

## State Compliance Comment

### **Observation No. 10: Prize Claims Should Be In Compliance With Rules**

#### *Observation:*

Lottery has not revised its administrative rules to reflect the Lottery's changing game structures. The Lottery pays claims for second-chance prizes without requiring the claimant to have physical possession of the winning ticket, in apparent conflict with N.H. Admin. Rules, Sw 602.01(a), which states, "No prize shall be paid without the physical possession of a winning ticket or valid subscription recorded in the lottery's central computer system."

In instant-ticket, second-chance drawings utilizing the Replay System apparatus, Lottery does not require winners to have physical possession of the winning ticket at the time the claim is filed. Lottery reports it does not consider the possession and presentation of a physical ticket necessary because players enter ticket validation information when entering the ticket into the Replay system prior to the drawing.

Lottery incorporates second-chance drawings in the prize structure of several instant-ticket games. Depending on the game, either all non-winning tickets or tickets reflecting a designated symbol enable the ticket holder to enter into a second-chance prize drawing at the conclusion of the game. Depending upon the game design, instructions on the back of the ticket direct the ticket holder to either mail or personally deliver the instant ticket to Lottery headquarters for entry into a manual drawing or to enter ticket information directly into Lottery's Replay website for a Lottery game with a second-chance prize Replay system drawing.

A similar observation was reported in the fiscal year 2010 audit management letter. Lottery, in its response to that comment, reported it was in the process of phasing out the use of the Replay system for second-chance Lottery drawings. However, Lottery's website reports Lottery conducted 15 second-chance drawings using the Replay system during fiscal year 2011, awarding a total of \$1,075,000 in prizes. Lottery did not address the recommendation to review the rules with legal counsel or request a clarification of the rule.

#### *Recommendation:*

Lottery should review with legal counsel whether its current practice of paying certain second-chance prizes without requiring the winner to present a winning ticket is in compliance with N.H. Admin. Rules, Sw 602, Prize Claims.

Lottery should consider whether N.H. Admin. Rules, Sw 602.01(a) should be clarified to describe the structure of the Lottery's games.

*Auditee Response:*

We concur. The Lottery discontinued the usage of the Replay program for the awarding of prizes, that are contained within the prize structure of an instant game, during the Fall of 2010. However, it has taken some time for the tickets printed prior to the change to end their selling period. The Lottery viewed the retrieval of the old tickets from the field as too costly and allowed the older tickets to sell through. The final drawing occurred in October of 2011, and there will be no more thereafter. We believe the issue is resolved going forward.

**Review Of Lottery Information Technology System General Controls**

As part of our financial audit of the Lottery for fiscal year 2011, we retained the services of a specialist to review the Lottery’s general controls over its significant information systems. The specialist’s review of Lottery’s systems for fiscal year 2011 was important given Lottery’s implementation of a new games management (gaming) system with a new system vendor on July 1, 2010.

The following comments result from the work of the information technology specialist engaged to perform the review of the Lottery systems. The comments include summary findings and Lottery management’s summary responses to the findings.

**Internal Control Comments - Information Technology - Significant Deficiencies**

**I. GENERAL COMMENTS**

**A. Software Change Control Failure** .....20  
**B. Independent Access To Vendor Source Data** .....21

**II. GOVERNANCE**

**A. Information Security Policies And Procedures** .....21  
**B. 2011 Multi-State Lottery (MUSL) Audit - Comments**.....22

**III. ACCESS TO PROGRAMS AND DATA**

**A. Logical Access**

1) Internal Control System (ICS System) Password Parameters .....23  
2) Default Internal Control System (ICS System) Account Password Change .....24

**B. System And Application Access Management And Monitoring**

1) Back Office System (BOS) Access Assignment .....24  
2) Access Termination .....25  
3) Periodic Review Of User Application Access .....25  
4) Virtual Private Network (VPN) Access .....26

**C. Change Management**

1) Change Management Policy .....27  
2) Bi-Monthly Meetings .....28  
3) Change Management Tracking .....29  
4) Internal Control System (ICS System) Vendor Segregation of Duties .....29

**D. Computer Operations**

1) Disaster Recovery And Business Continuity Plans .....30  
2) Service Level Agreement (SLA) Incident And Service Call Agreement And Compliance....30  
3) Service Call Statistics Source .....31

**Comments For Management Information**

**IV. PROCESS IMPROVEMENT OPPORTUNITIES**

**A. Vendor Independence**

1) Internal Control System (ICS System) Vendor Independence .....32

**B. Physical Security**

1) Relocation Of Internal Control System (ICS System) Server .....32

**Internal Control Comments**  
**Information Technology**  
**Significant Deficiencies**

**I. GENERAL COMMENTS**

**A. Software Change Control Failure**

*Observation:*

Following our fieldwork for the audit period under consideration, it was brought to our attention that during the Powerball draw of November 9, 2011, “draw sales” on the New Hampshire Lottery Commission (Lottery) internal control system (ICS system) did not balance with the NH gaming system. The gaming system indicated \$2.00 more in Powerball sales and \$1.00 more in PowerPlay sales than the ICS system. Investigations by Lottery and the gaming system vendor indicated the discrepancy was caused by an earlier incident on November 9, when during the software deployment of subscriptions wagers for the new Powerball matrix, the software for non-subscription wagers was accidentally introduced into the production system and nine (9) tickets for the new matrix and ticket cost were generated in the production system before the issue was identified and corrected.

While the imbalance was small in monetary terms and was caught by the reconciliation process, it raises questions about the adequacy of the game vendor’s controls over the testing, approval, and migration of software changes to the New Hampshire lottery system. While the gaming system vendor rightfully prides itself on being ISO9001 certified, ISO certification is very much focused on the adherence to documented standards and procedures, but not necessarily to the effectiveness of the documented procedures.

*Recommendation:*

It is recommended that Lottery with the support of the Department of Information Technology (DoIT) inquire of the gaming system vendor of what steps have been taken to ensure that similar failures are prevented in the future.

*Auditee Response:*

This occurrence was thoroughly reviewed and documented by the Lottery. In summary, the issue was caused by a software deployment error. To prevent the error from reoccurring, the vendor will not change the terminal software until the correct date.

## **B. Independent Access To Vendor Source Data**

### *Observation:*

During the audit period, Lottery was heavily reliant on data provided directly by the gaming system vendor, including statistics on retailer servicer calls, issues, and other events that could result in penalty payments to Lottery. Similarly, information pertaining to Lottery change requests are provided to Lottery by the vendor and not directly retrieved by Lottery from the vendor's database.

A lack of source data independence increases the risk that Lottery could be basing its estimation of vendor support effectiveness and its calculation of potential Service Level Agreement ("SLA") penalty payments on incomplete transaction populations. Additionally, the inability to review in totality all Lottery software changes in process restricts management's ability to provide due diligence oversight to the vendor's development process and increases the risk that unplanned or unexpected changes may be introduced.

### *Recommendation:*

As further discussed in Observations III. A and B on pages 23 and 24, it is recommended that Lottery gain direct access to the systems and data that would allow it to independently determine and monitor system performance and operation, including changes made to the systems and data pursuant to user change requests or outside of the user change request process.

### *Auditee Response:*

A formal access request has been submitted to the gaming system vendor for Lottery staff to have direct access of reconciled data - to be able to directly and independently calculate actual support call statistics.

## **II. GOVERNANCE**

### **A. Information Security Policies And Procedures**

#### *Observation:*

Lottery does not have a formally documented and approved security policy that provides guidance on information security for New Hampshire Lottery's environment that covers user interactions, applications, databases and the IT infrastructure.

Formal information security policies and procedures permit an Agency to introduce, promote and implement necessary controls with the authority of senior management.

*Recommendation:*

It is recommended that Lottery in co-operation with DoIT, develop, document, publish and enforce an appropriate information security policy that addresses the use, management and oversight of Lottery gaming and lottery systems, applications and data.

*Auditee Response:*

The Lottery is proactively enhancing its information security posture by participating in on-site monthly meetings with DoIT concerning the management and oversight of the Lottery's information technology resources, and will make recommendations to management as they deem necessary. Additionally, the Lottery Director of Security has been appointed to the State's Cyber Security Advisory Council, whose mission is to improve cyber security across the State of New Hampshire Government and its stakeholders by promoting awareness, developing effective policies and solutions, and obtaining supportive consensus for enterprise-wide initiatives that advance cyber security of information assets and technology resources.

**B. 2011 Multi-State Lottery (MUSL) Audit - Comments**

*Observation:*

The MUSL audit organization reviews Lottery compliance with MUSL requirements every two years. Self-assessments are required every other year. Several audit comments from the most recent MUSL audit in 2011 remained unresolved or lacked documentation to evidence resolution at June 30, 2011.

*Recommendation:*

It is recommended that Lottery continue in its efforts to resolve and adequately document its resolution of MUSL audit comments.

*Auditee Response:*

For informational purposes, the most recent MUSL Security Audit was the self-assessment conducted in September 2010.

Previously, in June 2010, MUSL conducted an on-site security and integrity review in support of the Lottery's conversion process which refers to the routine changeover of the gaming system from one vendor to another following the award of the state's on-line system gaming contract.

The finding of this review was presented to the MUSL Security and Integrity Committee (S&I) for their consideration to approve the process. On June 30, 2010, the S&I Committee accepted the review and voted in the affirmative to approve the Lottery's conversion to the new vendor on-line gaming system.

The Lottery is not at risk of sanction by MUSL; our efforts remain focused on the objective to continue to exceed minimum industry standards and goals established for security.

### **III. ACCESS TO PROGRAMS AND DATA**

#### **A. Logical Access**

##### ***1) Internal Control System (ICS System) Password Parameters***

###### *Observation:*

No official formal password policy for ICS system application is documented. Current ICS system password syntax is weak with a minimum password length of 6 characters with insufficient password history retained. The audit team was informed this was due to limitations in the ICS system application. The ICS system is used by Lottery to balance and prove ticket sales data from its gaming system.

Weak account and password controls increase the risk that unauthorized persons could gain access to sensitive systems and information. The risk to the Lottery is commensurate to the privileges associated with the account that may become compromised.

###### *Recommendation:*

It is recommended that Lottery management require the ICS system vendor to strengthen ICS password authorization controls and:

- create separate, unique and identifiable accounts for all persons with superuser privileges.
- reinforce with staff that have superuser account privileges to not share account credentials with other persons.
- support access requests to the server for the ICS system be logged by Lottery staff with a date, start and end time and reason (to be provided by the vendor before connection made). In the event the server for the ICS system is moved to the DoIT data center, no vendor connection should be made to the server without prior Lottery agreement.

###### *Auditee Response:*

Recommendation forwarded to the ICS system vendor on December 13, 2011 with instruction to report a timeline for completion.

## **2) Default Internal Control System (ICS System) Account Password Change**

### *Observation:*

The ICS system vendor was unable to provide evidence that the passwords used for internal default accounts within the ICS system database which support the ICS system application have been changed in accordance with best practices.

System accounts that retain default account names and passwords offer opportunities for unauthorized and undetected access to applications and their data assets by persons familiar with system defaults.

### *Recommendation:*

It is recommended that the Lottery management require the ICS system vendor provide evidence of default password change within the ICS system application and database or take steps to make changes to unchanged default passwords.

### *Auditee Response:*

Recommendation forwarded to ICS system vendor on December 13, 2011 with instruction to report a timeline for completion.

## **B. System And Application Access Management And Monitoring**

### **1) Back Office System (BOS) Access Assignment**

#### *Observation:*

Lottery's assignment of user access and privileges to the gaming system's BOS utilizes a cumbersome spreadsheet intended to identify and document user access rights. The gaming system vendor also uses the spreadsheet to establish user access and associated privileges in the BOS. The spreadsheet provides no clear references or aids to highlight potentially conflicting privileges. The BOS is used by the Lottery to administer its gaming system.

The inadequacy and lack of clarity of the access set-up spreadsheet in the management of user access to sensitive financial monitoring systems increases the risk that users may be granted unnecessary or inappropriate access rights that could compromise an appropriate segregation of duties.

#### *Recommendation:*

It is recommended that the Lottery management and the gaming system vendor review the current access set-up process, paying particular attention to improving the identification and avoidance of potential conflicts in assigned account privileges.

*Auditee Response:*

The Lottery and the gaming system vendor will review the access set-up process as recommended and request improvements that are technologically compatible with the vendor's system.

**2) Access Termination**

*Observation:*

Lottery management does not have a documented policy and procedure to ensure that terminated employee access to Lottery networks, systems and applications is removed in a timely manner.

The absence of a formal procedure to identify and remove in a timely fashion the access credentials of terminated employees increases the risk that unattended accounts could provide undetected gateways to key systems and data.

*Recommendation:*

We recommend that Lottery management develop, distribute, implement and enforce a formal policy and procedure to require that terminated employees are removed from the Lottery network, systems, and applications in a timely fashion.

*Auditee Response:*

The Lottery concurs with the recommendations and will work with the gaming system vendor to pursue these objectives.

**3) Periodic Review Of User Application Access**

*Observation:*

Lottery management does not perform a periodic review of persons with Lottery network and/or application access. Additionally, Lottery management has not conducted a review of user Lottery application privileges to ensure that an appropriate segregation of duties is being managed.

The absence of periodic management reviews of the network and key application user access increases the risk that accounts belonging to terminated staff may provide an intruder with an undetected gateway to the system and active staff may retain processing capability that exceeds their job requirements, undermining a prudent segregation of duties.

*Recommendation:*

We recommend that Lottery management:

- require the gaming system vendor to provide Lottery management with the capability to generate periodic (every 3-6 months) reports of current Lottery user access and application privileges assigned to the user-ID accounts.
- review the report and take steps to remove network and/or systems access to unauthorized persons.
- review the report and take steps to remove unnecessary or inappropriate application access privileges.

*Auditee Response:*

The Lottery concurs with the recommendations and will work with the gaming system vendor to pursue these objectives.

**4) *Virtual Private Network (VPN) Access***

*Observation:*

Lottery and vendor VPN user access is not reviewed periodically.

Without periodic reviews of Lottery and vendor users granted remote access privileges, terminated staff or persons whose job duties may have changed could retain remote access to important networks, systems, and applications that is no longer required or appropriate.

*Recommendation:*

It is recommended that Lottery management require DoIT to conduct periodic reviews of users who have access to Lottery networks or systems and provide Lottery management with a quarterly report of review results.

*Auditee Response:*

DoIT reviews state employee VPN access on a 90 day cycle; the Lottery will work with the gaming system vendor to establish an annual review of vendor VPN access users.

## **C. Change Management**

### ***1) Change Management Policy***

#### *Observation:*

Lottery was unable to provide a documented Change Management Policy that describes the requirements, processes and approvals required when requiring changes to be made to the Lottery's gaming and financial management operations systems and applications.

The absence of a formal and enforced Lottery Change Management Policy that documents steps to be followed, approvals required, testing to be conducted, and acceptance sign-offs to be required increases the risk that untested, unauthorized, and/or inappropriate software changes could be put into production.

#### *Recommendation:*

It is recommended that Lottery work with both the internal control system vendor and the gaming system vendor to document and introduce a common Change Management policy and procedure that defines the software change management process from initiation through migration to production and documents the roles and responsibilities of all parties including the owners of development, testing, and migration.

#### *Auditee Response:*

Section 3.4-3.4.17:

“RFP 17. Configuration Management. The Successful Vendor shall operate under a defined procedure for changes to documentation, procedures, specifications, program source and object code, and other major System components. Strict performance according to principles of configuration management is required.

The gaming system vendor's change control and configuration management procedures are well documented and ISO 9000 certified. The gaming system vendor has also been certified for its Information Security Management System (ISMS) against the requirements of the international standard ISO27001:2005.

The gaming system vendor only operates under strictly defined change control and configuration management procedure practices utilizing Microsoft's Visual Source Safe to track not only software changes, but also to track changes in manuals, procedure, and configuration files.

The gaming system vendor agrees that configuration management practices apply to all of the following components: documentation, procedures, specifications, program application source and object code, Operating Systems, database platforms, other third-party applications, Host Systems network hardware and major hardware components, and any other major System components.”

*LBA Rejoinder:*

It is important that Lottery becomes more involved in the change management control process to lessen the risk that changes intended by the gaming system vendor to fix problems or improve efficiencies do not result in unintended problems at the Lottery, such as the instance described in General Comment I.A on page 20.

**2) Bi-Monthly Meetings**

*Observation:*

Bi-monthly meetings and/or conference calls between Lottery, the gaming system vendor and the internal control system vendor are informal, and are not documented with meeting minutes. As such, decisions and agreements supposedly made at prior meetings are not supported by documented evidence.

Informal meeting procedures for complex relationships risk unproductive use of time, misunderstanding of critical issues across groups, miscommunication of important decisions leading to agreements not being implemented or followed-up in a timely fashion.

Without meeting minutes, there is no historical record of agreements and decisions made that can help in completing tasks timely, or resolve future disputes or disagreements between parties.

*Recommendation:*

It is recommended that Lottery management require a more formal approach to bi-monthly inter-group meetings. In particular, it is recommended that:

- a pre-published and distributed agenda be prepared for all formal meetings.
- detailed minutes be kept for all formal meetings, including attendance, issues discussed, decisions made (persons responsible and target dates), and open and closed items.
- meeting minutes be distributed in advance of the next meeting for review by each management group.
- meeting minutes be filed for future reference through the life of the relationship.

*Auditee Response:*

All recommendations are in place and are currently being followed.

### **3) Change Management Tracking**

#### *Observation:*

Lottery does not have the ability to extract all New Hampshire related software change data from the gaming system vendor's Test Tracker application, which is used to document gaming system vendor software change development and migration progress. Lottery was only able to view or take screen prints, one page at time.

The inability to directly query and extract a full population of Lottery related software changes from the Test Tracker system increases the risk that Lottery may miss software changes that could have an impact on the Lottery's gaming operation and restricts Lottery's ability to monitor the change management process.

#### *Recommendation:*

It is recommended that Lottery management require the gaming vendor to provide Lottery with the capability to independently run report queries and data extractions for all Lottery related software changes directly from the Test Tracker system.

#### *Auditee Response:*

A formal access request has been submitted to the gaming system vendor for Lottery staff to independently run report queries and data extractions for all related software changes from the Test Track Web Application.

### **4) Internal Control System (ICS System) Vendor Segregation of Duties**

#### *Observation:*

The ICS system vendor was unable to provide evidence that an adequate segregation of duties exists between ICS system developers and production software migrators.

An inadequate separation of duties increases the risk that software developers may be able to introduce unapproved or unauthorized software changes into production.

#### *Recommendation:*

It is recommended that Lottery require the ICS system vendor to provide evidence of an appropriate segregation of duties between software development staff and those responsible for migrating ICS system software into the Lottery production environment. Alternatively, the ICS system vendor should provide documented evidence that mitigating controls have been put in place to reduce risk of inappropriate migration activity.

*Auditee Response:*

Recommendation forwarded to the ICS system vendor on December 13, 2011 with instruction to report a timeline for completion.

**D. Computer Operations**

***1) Disaster Recovery And Business Continuity Plans***

*Observation:*

Interviews with State of New Hampshire Department of Information Technology (“DoIT”) management, and Lottery indicated that the Lottery Disaster Recovery Plan (“DRP”) dates from 2008 and reflects the infrastructure, applications and processes used with the prior third party gaming service provider.

The lack of a comprehensive and tested Disaster Recovery Plan (DRP) and complementary Business Continuity Plan (BCP) increases the risk that in the event of a serious environmental event affecting Lottery’s gaming operations, including the balancing and reconciliation of gaming operations, could be seriously disrupted.

*Recommendation:*

It is recommended that Lottery in cooperation with DoIT and its gaming system and internal control system vendors take action to make the DRP current and augment it with an appropriate Business Continuity Plan (“BCP”). It is further recommended that the DRP and its associated BCP be treated as living documents subject to ongoing revision and annual testing.

*Auditee Response:*

Lottery/DoIT are in the process of planning work sessions for the first quarter of 2012 that will lead to the completion of the revised DRP with input from the gaming system and ICS system vendors.

***2) Service Level Agreement (SLA) Incident And Service Call Agreement And Compliance***

*Observation:*

Service and support calls provided by the gaming system vendor are reviewed by Lottery against a SLA checklist for potential penalty implications. However, it was not clear if the gaming system vendor service call and incident SLAs are formally defined, clearly documented, and agreed and accepted by both parties.

Without clear agreement on properly documented SLAs and certainty of full populations of incident and service calls, calculations of potential vendor penalties may be incomplete and inaccurate.

*Recommendation:*

It is recommended that the Lottery management work with the gaming system vendor to clearly document contractual SLAs and potential penalties for failing to meet SLAs. We further recommend that the agreed SLAs be reviewed periodically to ensure that they remain appropriate.

*Auditee Response:*

Lottery currently reviews all SLAs and addresses any errors and changes with the gaming system vendor that could potentially result in additional penalties.

**3) Service Call Statistics Source**

*Observation:*

Retailer service call statistics received and managed by the gaming system vendor are provided to Lottery by that vendor.

Without the ability to review the call database independently, there is a risk that Lottery may not be receiving a full population of calls resulting in inaccurate tracking and measurements against agreed SLAs resulting in underpaid penalties.

*Recommendation:*

We recommend that the Lottery management request direct access to the BOS system or some sub-set of reconciled data to be able to directly and independently calculate actual support call statistics that could result in penalty payments against agreed SLAs.

*Auditee Response:*

A formal access request has been submitted to the gaming system vendor for Lottery staff to have direct access of reconciled data to be able to directly and independently calculate actual support call statistics.

## Comments For Management Information

### **IV. PROCESS IMPROVEMENT OPPORTUNITIES**

#### **A. Vendor Independence**

##### ***1) Internal Control System (ICS System) Vendor Independence***

*Observation:*

The software vendor used by Lottery to provide critical ICS system software to reconcile gaming system activity is contracted to the gaming system vendor and not Lottery.

The fact the ICS system vendor provides service to Lottery pursuant to a contract with the gaming system vendor rather than Lottery could potentially lead to a conflict of interest in any dispute related to reconciliation of the gaming system activity.

*Recommendation:*

It is recommended that Lottery management assess potential risk and if deemed appropriate give consideration to contracting directly for ICS services rather than obtaining those critical control services through the gaming system vendor.

*Auditee Response:*

The current contract for the online gaming vendor requires that the vendor supplies an internal control system that is independent, as it has been since 1995 in each contract.

#### **B. Physical Security**

##### ***1) Relocation Of Internal Control System (ICS System) Server***

*Observation:*

The production server for the ICS system is located in the Lottery Operations room. When the ICS system vendor requires access to provide application support, they access the ICS system via a Virtual Private Network (VPN) connection. Lottery Operations staff physically connect the Ethernet cable to facilitate the connection. The room has a closed circuit television camera (CCTV) mounted.

Key production equipment should be appropriately physically and environmentally secured. Without a data center environment and security, the production server may be victim of rodents, wire destruction, and interruption of service.

*Recommendation:*

It is recommended that Lottery management work with DoIT to move the server and cabinet to the data center and route access through an appropriate server. The relocation would secure and protect the equipment, provide the ICS system vendor with secured access via VPN as required, and facilitate a forensic audit trail of access.

If the server is not moved, the effectiveness of the security camera should be further considered. While there is a security camera installed in the office containing the server for the ICS system, recording does not occur unless there are lights. Additionally, by its nature the camera is a detective control, i.e. records during the event and does not provide preventative security, i.e. set off an alarm.

Intruders (including local wildlife) are most likely to attempt to gain access at night when the CCTV is likely to be of limited use.

It is recommended that Lottery management, in addition to a recording camera, also install an alarmed motion detector in the room that hosts the server for the ICS system.

*Auditee Response:*

The office containing the server for the ICS system has a door with an alarm fitted.

The option of moving the ICS server to the computer room would conflict with the section of MUSL Rule 2 concerning ICS lock down procedures.

Although Lottery staff cannot recall an incident that involved damage to equipment by wildlife, the building owner arranges for preventative pest control services as may be recommended by pest control professionals.

**THIS PAGE INTENTIONALLY LEFT BLANK**

## APPENDIX

### Current Status Of Prior Audit Findings

The following is a summary of the status, as of December 21, 2011, of the observations contained in the New Hampshire Lottery Commission Management Letter for the fiscal year ended June 30, 2010. That report can be accessed at, and printed from, the Office of Legislative Budget Assistant website: <http://www.gencourt.state.nh.us/LBA/AuditReports/financialreports.aspx>.

#### Status

#### *Internal Control Comments*

##### *Material Weakness*

- |   |   |   |   |
|---|---|---|---|
| 1. Risk Assessment Should Be Performed ( <i>See Current Observation No. 5</i> ) | ● | ○ | ○ |
|---|---|---|---|

##### *Significant Deficiencies*

- |  |   |   |   |
|--|---|---|---|
| 2. Controls Over Lottery's Assets Should Be Strengthened   | ● | ● | ● |
| 3. Compliance With Financial Control Activities Should Be Improved ( <i>See Current Observation No. 3</i> )        | ● | ○ | ○ |
| 4. Replay Program Should Be Fully Documented ( <i>See Current Observation No. 6</i> )                              | ○ | ○ | ○ |
| 5. Appropriateness Of Instant Ticket Revenue Collection Policies And Procedures Should Be Reviewed                 | ● | ● | ● |
| 6. Only Advertising Costs Should Be Charged To Advertising Accounts  | ● | ● | ● |
| 7. Policies And Procedures For Accessing The Draw Room Should Be Expanded ( <i>See Current Observation No. 1</i> ) | ● | ○ | ○ |
| 8. Access Controls Should Be Improved ( <i>See Current Information Technology Comments III. A, 1 and 2</i> )       | ○ | ○ | ○ |

#### *State Compliance Comments*

- |   |   |   |   |
|---|---|---|---|
| 9. Tax Status Of Tri-State Lotto Prizes Should Be Determined                                  | ● | ● | ● |
| 10. Prize Payment Rules Should Be Followed  | ● | ● | ● |
| 11. Prize Claims Should Be In Compliance With Rules ( <i>See Current Observation No. 10</i> ) | ● | ● | ○ |

#### Status Key

				<u>Count</u>
Fully Resolved	●	●	●	5
Substantially Resolved	●	●	○	1
Partially Resolved	●	○	○	3
Unresolved	○	○	○	2

**THIS PAGE INTENTIONALLY LEFT BLANK**