INFORMATION SYSTEMS AUDIT

Montana Lottery Security

Department of Administration

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:

http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
James Gillett
Angie Grove

September 2010

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of security at the Montana Lottery. Montana law requires the Legislative Audit Division to perform a comprehensive security audit of the Montana Lottery every two years. We reviewed the 18 security areas defined in statute.

This report contains five recommendations for strengthening controls including: change control, ticket activation, ineligible players, paying winners, and access.

We wish to express our appreciation to the Montana Lottery for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

TABLE OF CONTENTS

Figures and Tables

Figures

Appointed and Administrative Officials

Montana Lottery	George Parisot, Director
	John Tarr, Security Director
	Paul Gilbert, Information Technology Services Director
	Armond Sergeant, Accounting Services Director
Department of Administration	Janet R. Kelly, Director
Lottery Commission	Robert Crippen, CPA, Chair, Butte
	Craig Anderson, Sheriff, Glendive
	Thomas M. Keegan, Attorney at Law, Helena
	Beth O'Halloran, Missoula
	Wilbur Rehman, Helena

MONTANA LEGISLATIVE AUDIT DIVISION
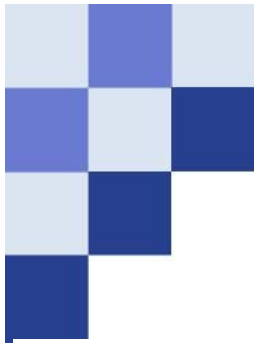
INFORMATION SYSTEMS AUDIT

Lottery Security
Montana Lottery

Lottery generated over $10 million in revenue for fiscal year 2009 from ticket sales, so it is critical for operations to maintain strong security controls.

Context

The Montana Lottery was created in 1987 and its operations are funded by the sale of lottery tickets. Lottery ticket categories include: scratch tickets and online tickets. Revenue is generated either through the sale of individual tickets or by retailer purchases of scratch ticket packs for sale throughout Montana. Online game tickets are sold at participating retailers via terminals. Net revenues from both types of ticket sales are transferred to Montana's general fund.

Montana law requires the Legislative Audit Division to perform a comprehensive security audit of the Montana Lottery every two years. We reviewed the 18 security areas as defined in §23-7-411, MCA. Testing included evaluating Lottery against Montana statute, Multi State Lottery Association (MUSL) regulations, Montana Lottery internal security procedures, statewide information technology policies, and industry best practices.

Results

Overall, security controls are in place in the areas outlined by statute; however, we identified areas where controls can be strengthened. Areas for improvement include change control, access and Lottery business processes.

Lottery maintains an Internal Control System (ICS) which records and reports Lottery sales and drawings information for all games. The system is used to ensure sales information is accurate prior to all MUSL and Montana Lottery draws. Our review determined ICS changes were not tested in a test environment. Changes were introduced directly to the production environment, which could result in serious consequences for the system.

Scratch tickets must be electronically activated in order to be redeemable. We determined individuals with the ability to activate scratch tickets also had physical access to the scratch ticket inventory. This creates the potential for these individuals to obtain and activate scratch tickets without secured oversight.

By law, certain individuals are not eligible to play the Lottery. A procedure has been implemented to check for ineligible players; however, due to a weak system control, an ineligible player may be paid for a winning ticket. We also noted a control issue with payments made via electronic funds transfer. The current system could allow an individual to submit an unauthorized or incorrect request to the State Treasury. Finally, we noted an unsecure key storage issue related to a new type of self service Lottery ticket machine. Uncontrolled access to these machines could allow individuals access which is not appropriate to their job duties.

Recommendation Concurrence	
Concur	5
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

Chapter I – Introduction and Background

Introduction

The Montana Lottery was created in 1987 and its operations are funded by the sale of lottery tickets. Lottery tickets are sold to various retailers throughout Montana. Revenue is generated either through the sale of individual tickets or by retailer purchases of scratch ticket packs.

Lottery ticket categories include: scratch tickets and online tickets. Scratch tickets contain predetermined winners. The ticket purchaser must scratch off a covering in the play area. Winning tickets under $600 can be validated and paid by a Lottery retailer. If the winnings are $600 or more, the winning ticket must be validated and paid at the Lottery headquarters in Helena. Tickets of any value can be claimed by mail at the Lottery headquarters.

Online game tickets are sold at participating retailers via terminals. Winners are determined through drawings held throughout the week and are paid out similar to scratch tickets. Net revenues from both types of ticket sales are transferred to Montana's general fund. Lottery transferred net revenues of $10.1 million to the general fund for fiscal year 2009.

Audit Scope and Objective

Montana law requires the Legislative Audit Division to perform a comprehensive security audit of the Montana Lottery every two years and specifically defines areas to be included. We reviewed the 18 security areas as defined in §23-7-411, MCA:

- personnel security
- lottery sales agent security
- lottery contractor security
- security of manufacturing operations of lottery contractors
- security against ticket or chance counterfeiting and alteration and other means of fraudulently winning
- security of drawings among entries or finalists
- computer security
- data communications security
- database security
- systems security
- lottery premises and warehouse security

- ◆ security in distribution
- ◆ security involving validation and payment procedures
- ◆ security involving unclaimed prizes
- ◆ security aspects applicable to each particular lottery game
- ◆ security of drawings in games whenever winners are determined by drawings
- ◆ the completeness of security against locating winners in lottery games with preprinted winners by persons involved in their production, storage, distribution, administration, or sales
- ◆ any other aspects of security applicable to any particular lottery game and to the lottery and its operations

Our objective was to determine whether Lottery has controls in place over all eighteen security areas.

Methodology

To accomplish our objective, we performed work under each statutorily defined area. Work included interviews with agency and vendor personnel, observation of facilities and systems in place for Lottery and its vendors, testing of identified controls, and review of agency and vendor policies and procedures.

More specifically, testing included evaluating Lottery against Montana statute, Multi State Lottery Association (MUSL) regulations, Montana Lottery internal security procedures, statewide information technology policies, and industry best practices. We observed daily operations, obtained input from key personnel, and reviewed associated documentation. We reviewed employee and contractor procedures, evaluated employee and contractor access to facilities, systems, and data, and observed ticket stock distribution procedures and identified controls. Finally, we reviewed computer systems and network configurations and system reports.

This audit was conducted in accordance with government auditing standards published by the United States Government Accountability Office.

Prior Audit Recommendations

Legislative Audit Division Information Systems auditors conducted a similar audit in 2008 which resulted in a management memorandum with suggestions for strengthening controls. Our work for this audit included reviewing concerns outlined in the memorandum and determining if our suggestions had been incorporated into Lottery business processes.

CONCLUSION

Overall, security controls are in place in the areas outlined by statute; however, we identified areas where controls can be strengthened. Areas for improvement include change control, access and Lottery business processes.
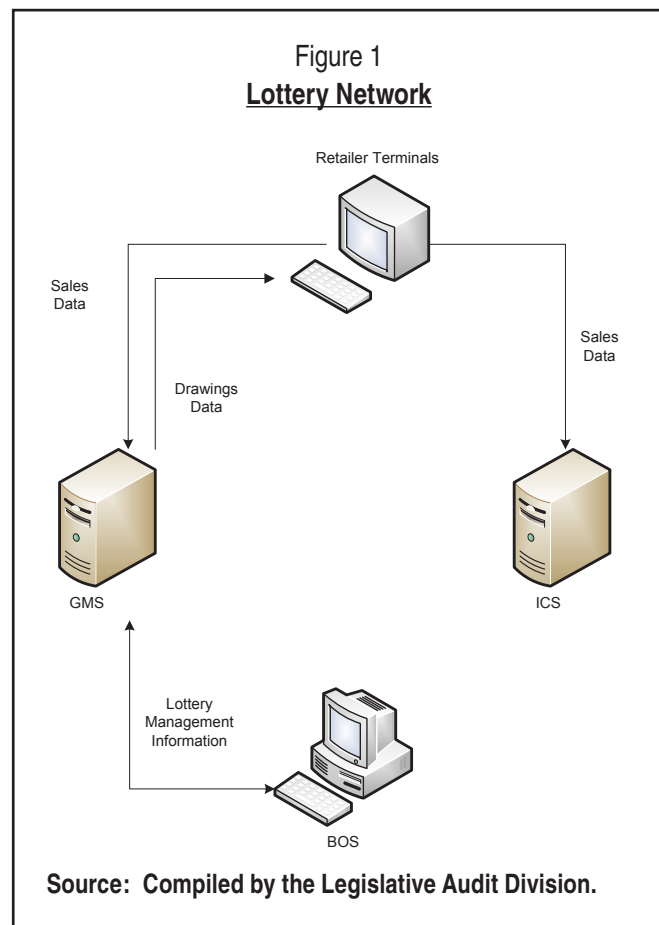
Chapter II – Findings and Recommendations

Introduction

The Montana Lottery is a member of the Multi State Lottery Association (MUSL), a nonprofit association owned and operated by its member lotteries. Each member offers one or more lottery games administered by MUSL. Montana participates in online MUSL games which generate additional revenue from popular large prize games such as Powerball and Mega-millions. MUSL is governed by a Board of Directors comprised of one representative from each of the member states. The Board develops MUSL rules and regulations to be followed by all participating state lotteries. Montana Lottery operations are governed by statute, MUSL rules, State information technology policy, and internal security policies.

MUSL requires member lotteries to operate a games management system (GMS) to manage both online and scratch games and an Internal Control System (ICS) as a check and balance against ticket sales recorded in the GMS. Montana's GMS is currently operated by a third party vendor. The vendor developed, maintains, and operates the GMS as well as installing and maintaining sales terminals at retailer locations throughout the state. The ICS was developed and is maintained by a separate third party vendor. The ICS also records all Lottery sales and drawings information and is used to ensure the GMS is reporting accurately. Lottery personnel interface with the GMS through a separate application called the Back Office System (BOS). Lottery manages its sales, marketing, and claims information contained in the GMS through BOS. The figure shows the interaction between the systems within the lottery network.

Figure 1
Lottery Network

Retailer Terminals

Sales Data

Sales Data

Drawings Data

GMS

ICS

Lottery Management Information

BOS

Source: Compiled by the Legislative Audit Division.

Along with each of these systems, we reviewed business processes in place at Lottery to identify controls which enable compliance with statute, MUSL rules, State policy, and industry best practices. This report contains five recommendations for strengthening controls including change control, scratch ticket activation, screening for ineligible players, processes for paying winners, and access to the new Winstation terminals.

ICS Change Control

The ICS records and reports Lottery sales and drawings information for all games. The system is used to ensure sales information is accurate prior to all MUSL and Montana Lottery draws. Sales information is used to establish drawing prize amounts and identify winning tickets once the draws have been completed.

MUSL rules state "any changes to the ICS software, operating system or hardware must be tested in a test environment that is separate from the production environment prior to implementation." We reviewed one year of ICS changes and determined changes were not tested in the testing environment. Information provided by Lottery showed all changes were introduced directly to the ICS production environment.

Changes introduced directly to the production environment can have serious consequences including disabling a computer system. ICS failures could, at a minimum, delay a MUSL drawing or, at worst, prevent Montana from participating in MUSL games, such as Powerball or Mega-millions, due to noncompliance with MUSL rules. In 2009, these games accounted for 38 percent of revenue for the Montana Lottery.

Lottery management asserted, under its previous ICS vendor contract, no test environment existed and procedures did not require testing in a nonproduction environment. However, when a new vendor was contracted for ICS development and maintenance, Lottery management implemented new procedures requiring all major changes to ICS be tested in the test environment. According to management, the changes we reviewed were all minor changes and did not require testing in the test environment. Industry standards state that organizations should test, validate, and document changes to the information system before implementing the changes on the production system. Additionally, the MUSL rule states "any" change must be tested prior to deployment in the production environment.

MUSL also requires changes to the ICS operating system or application to be thoroughly documented. Industry best practices provide guidance for the change control process and recommends an organization provide a standardized process to document changes. Documentation should note the nature of the request and ensure the changes are categorized, prioritized, and authorized. Our review of ICS change

documentation identified no process of prioritization and not all documentation included authorizations. Under the current change control process Lottery relies on an informal exchange of information with the ICS vendor, including e-mail and other forms of documentation. No standardized change control documentation was in use. Reliance on nonstandardized change control documentation can make it difficult, if not impossible, to correct errors made as a result of programming or system changes. The Lottery might be unable to identify what specific changes were made, when they were made, or who allowed the change, thus complicating the task of correcting an error.

___

RECOMMENDATION #1

We recommend the Montana Lottery strengthen the Internal Control System change control process by:

A.   *Requiring all changes be tested in the test environment prior to implementation in accordance with Multi State Lottery Association rules and industry standards.*

B.   *Ensuring change control documentation is complete.*

___

Activation of Scratch Tickets

A specific process must occur for scratch tickets to be redeemable. This activation process allows a ticket to be cashable. The primary responsibility for ticket activation rests with the retailers; however, according to Lottery management, retailers often sell tickets without activating them first. Without being activated, a winning ticket cannot be cashed. Winning tickets can be taken to different retailer locations for cashing, but tickets can only be activated by the retailer who sold the ticket.

A limited number of Lottery personnel have access to remotely activate scratch tickets. This access is needed to assist retailers who have sold nonactivated tickets. We determined this access to computer system functions was given to individuals who also have 24 hour physical access to the secure storage location of scratch tickets. Access to the ticket storage area is recorded in the building security system; however, the individuals monitoring access are the same individuals who have physical access. Additionally, there is no video monitoring of the storage area. This dual access could allow Lottery personnel to enter the secure storage area, obtain scratch tickets, and activate them without secured oversight.

Information technology standards state an organization should establish a division of responsibilities and separate duties to eliminate conflicts of interest. One method of

creating this separation is through segregation of duties between physical scratch ticket access and assigned system access. Lottery's lack of segregation between physical and computer system access without independent monitoring could allow unauthorized distribution and/or use of activated scratch tickets. Lottery management asserts this access has existed for years. Additionally, Lottery management stated that segregating these abilities would be difficult as they need to be able to assist retailers at all times of the day. Management was also concerned reassigning the system access to different individuals would create an access overlap somewhere else. However, we believe it is essential Lottery management identify a way to segregate physical and system access. This could be achieved by assigning the system access to individuals who already have access to BOS but do not have physical access to scratch tickets.

RECOMMENDATION #2

We recommend the Montana Lottery segregate the ability for Lottery personnel to physically access scratch tickets from the ability to electronically activate the tickets.

Ineligible Players

Per Montana statute §23-7-302(4), MCA, individuals holding certain positions are not eligible to play the Lottery. While this statute requires individuals to abstain when they are not eligible, Lottery maintains a list of names of ineligible players within the games management system. Any winning ticket over $599.99 must be claimed at, or mailed to, Lottery headquarters. Claimants must also complete and submit a claim form to the Lottery. During the claim process, the GMS checks the claimant name against the database of ineligible players. If the claimant is on the list, the system generates a visible alert stating the individual is ineligible and to contact security. Lottery personnel should then notify security who confirms the claimant is the same as the person named on the notification and determines if they are still ineligible to play. However, the system allows a user to ignore the notice and continue processing without the approval of Lottery security.

Due to a weak system control, an ineligible player may be paid for a winning ticket. Lottery management stated the system was never programmed to prevent this from occurring. The system was programmed to make the check, and issue a warning, but not to prevent the process from continuing. The statute does not require Lottery to perform this check. However, since Lottery has taken the time and effort to develop a tool, it should strengthen the tool to make it more effective in preventing ineligible players from claiming Lottery prizes.

Payments via Electronic Funds Transfer

Individuals claiming a winning ticket can request to have the prize paid by check or directly to a bank account via electronic funds transfer (EFT). Payments by check are created in the GMS and linked directly to a winning ticket which has been scanned into the system. A record is created with the check number and ticket number, and the check is printed from the GMS. Winners selecting the EFT payment make their choice on the claim form and Lottery personnel complete an EFT form to be sent to the State Treasury. The EFT form contains both a line designating who is requesting the EFT and a line for the requester's signature. These forms were developed by the State Treasury and are completed manually by Lottery personnel.

During our review, we noted the EFT forms can be submitted to the State Treasury without a requester signature and without having been reviewed by a second Lottery staff member. Additionally, unlike checks, the EFT form and payment are not directly linked to a winning ticket within the Lottery GMS. Instead, Lottery relies on staff to make photocopies of the winning ticket and associated claim form and file them with the EFT form.

According to State policy, "there are four kinds of functional responsibilities that should be performed by different work units, or at a minimum, by different persons within the same unit". Three of the four duties are: authorization to execute transactions, recording transactions, and periodic reviews and reconciliation of existing assets to recorded amounts. Further, the policy states individuals who prepare/record checks should not also sign the checks or reconcile the accounts. In our opinion, an EFT is an electronic check. The State Treasury relies on controls in place at the agency level to ensure EFT requests are authorized.

Lottery's lack of a secondary review and the inability to link the EFT payment to a winning ticket in the GMS could allow an individual to submit an unauthorized or incorrect EFT request to the State Treasury. Additionally, the lack of routine reconciliation does not allow the Lottery to detect any unauthorized EFT. For example, we reviewed an EFT form where the account information had been changed

by hand and no requester signature appeared on the form. Therefore, Lottery staff could mistakenly issue an EFT to the wrong person or account. Lottery personnel could also intentionally issue an EFT payment to themselves or another unauthorized individual.

Lottery management stated personnel should be signing the EFT form and generally they obtain a secondary review. However, no formal policy exists to mandate the requestor sign the document and obtain a secondary review and sign-off prior to sending the request to the State Treasury. Lottery staff stated EFTs are not managed in the GMS due to a technical issue that resulted in recording of duplicate payments. However, the fact that the GMS has a process which allows for recording EFTs indicates Lottery intended to be able to record these payments in the system. Correcting the technical problem will allow Lottery to record EFTs in a manner similar to checks.

While State policy requires agencies to reconcile payments to documentation; during our review, we were not made aware of any routine reconciliation of the EFT documentation, including winning tickets, to payments issued. The State Treasury does not require the forms to be signed; rather, they will accept forms from an authorized requester via e-mail.

RECOMMENDATION #4

We recommend the Montana Lottery strengthen controls over the electronic fund transfer process by:

A.   *Recording electronic fund transfers in the game management system.*

B.   *Conducting ongoing reconciliation of all payments via electronic funds transfer.*

Winstation Keys

Lottery, in conjunction with its vendor, has developed a new self service machine which allows players to purchase both online and scratch game tickets. These new Winstations started being installed at retailers throughout Montana, at the time of our review. Winstation access is controlled through sets of physical keys. One set is given to the retailer for ticket restocking and collection of cash. The other set is sent to Lottery headquarters for safekeeping in the event a retailer loses one or more of the keys.

During our review we noted keys sent to the Lottery were being stored in an unsecure cabinet in the Lottery security office. The security office is generally kept unlocked with the door open allowing other Lottery personnel uncontrolled access. Additionally, Lottery maintains a Winstation in its headquarters lobby. The primary keys for the Lottery Winstation are split between two office sections of the Lottery; however, in each instance we determined the keys were stored in unsecured locations allowing access by all Lottery personnel.

Industry standards require organizations establish a division of responsibilities and separate duties to eliminate conflicts of interest. Uncontrolled access to the Winstation keysets could allow individuals to have access not appropriate to their job duties. Improper segregation of duties could result in keys being removed from the Lottery without authorization and used to access the Winstations at retailer locations or Lottery headquarters. This could include gaining access to the cash receptacles.

Lottery has developed draft security policies for both the retailer and Lottery Winstation keys. However, these policies were neither implemented nor communicated to Lottery personnel prior to the installation of Winstations at retailers and the Lottery. In addition, our review of the draft policies identified areas needing improvement in the language regarding segregation of duties surrounding the storage of and access to Winstation keys.

RECOMMENDATION #5

We recommend the Montana Lottery implement Winstation key control policy and procedures addressing:

- *Storage*
- *Access*
- *Segregation of duties*

MONTANA LOTTERY

LOTTERY RESPONSE

Montana LOTTERY
For the fun of it! 2525 N. Montana, Helena, MT 59601 • P: 406-444-5825 • F: 406-444-5830

September 9, 2010

Ms. Tori Hunthausen
Legislative Auditor
Office of the Legislative Auditor
State Capital Building
Helena, MT   59620-1705

Subject: Response to 2010 Montana Lottery Security Audit

Dear Ms. Hunthausen:

Thank you for the opportunity to respond to the report on Montana Lottery Security dated
August 26, 2010. The Montana Lottery concurs with the audit findings and recommendations.
We have or will take the necessary action to comply with all recommendations.

The following is our response to specific recommendations of our audit team.

RECOMMENDATION #1

**We recommend the Montana Lottery strengthen the Internal Control System change
control process by:**

    **A. Requiring all changes be tested in the test environment prior to implementation in
        accordance with Multi State Lottery Association rules and industry standards.**
    B. Ensuring change control documentation is complete

We concur and have implemented procedural and policy changes in response to this
recommendation. The Lottery Information Systems Director will assume responsibilities for
monitoring compliance within these areas.

RECOMMENDATION #2

**We recommend the Montana Lottery segregate the ability for Lottery personnel to
physically access scratch tickets from the ability to electronically activate the tickets.**

We concur and have implemented software and procedural changes in response to this recommendation and have moved this ability from a Security function to an Accounting function since Accounting personnel have no access to bulk scratch tickets inventory.

RECOMMENDATION #3

We recommend the Montana Lottery strengthen games management system controls to prevent processing of ineligible player claims.

We concur and will implement software changes in response to this recommendation. After testing we expect the requested changes to be fully implemented by January 2011. In the interim, we have established physical procedures, which require dual review of a suspected ineligible players claim.

RECOMMENDATION #4

We recommend the Montana Lottery strengthen controls over the electronic fund transfer process by:

    A. Recording electronic fund transfers in the game management system.
    B. Ongoing reconciliation of all payment via electronic funds transfer.

We concur and will work with our Lottery gaming management system vendor INTRALOT to develop a software change to record these EFT transfers in GMS. We have requested changes to the system to allow documentation of EFT transfers and expect this to be fully implemented by January 2011. In the interim, we have implemented an internal control policy change in accounting that now requires two employees physically review and sign off on all EFT transfers.
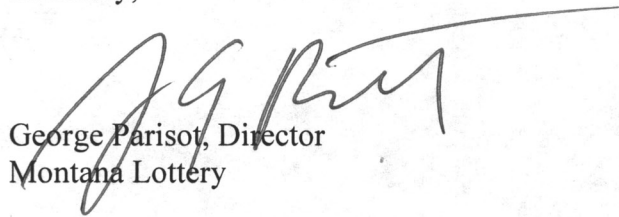
RECOMMENDATION #5

We recommend the Montana Lottery implement WIN Station key control policy and procedures addressing:

-Storage
-Access
-Segregation of duties

We concur and have implemented policy and physical changes in response to this recommendation. Procedures are now in place which require all spare keys received be logged into a software database and then stored in a dual security cabinet with one key held in Security and one key held in Accounting.

Thank you again for the opportunity to respond.   Your team established a good rapport with our office and showed strong professional knowledge and personal professionalism while working in our area. Please express my appreciation to your staff for their efforts in conducting this audit.

Sincerely,

George Parisot, Director
Montana Lottery