Legislative Audit Division

State of Montana

Report to the Legislature

September 2003

Information System Audit

Montana Lottery Security

Department of Administration

This report contains information regarding the security controls over Montana Lottery operations. The report contains nine network, computer, and general security recommendations addressing areas where the Montana Lottery can improve security over the Montana Lottery operations.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

03DP-03

INFORMATION SYSTEM AUDITS

Information System (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. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

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

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.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb	Representative Dee Brown
Senator Mike Cooney	Representative Tim Callahan
Senator Jim Elliott, Vice Chair	Representative Hal Jacobson
Senator John Esp	Representative John Musgrove
Senator Dan Harrington	Representative Jeff Pattison, Chair
Senator Corey Stapleton	Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

September 2003

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our security audit over the operation of the Montana Lottery. The report concludes that Lottery operates in compliance with federal tax withholding requirements; security controls exist but can be improved to ensure security over Lottery operations; and procedures can be improved to comply with internal policies and procedures. The report includes nine recommendations and the Lottery response to the audit report is contained at the end of the report.

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

Respectfully submitted,

Signature on File

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@state.mt.us

Legislative Audit Division

Information System Audit

Montana Lottery Security

Department of Administration

Members of the audit staff involved in this audit were David P. Nowacki, Ida L. Sajor, and Jessica Solem.

Table of Contents

Appointed and Administrative Officials

Montana Lottery Commission	Robert Crippen, Chair	Butte
	Clifford Brophy	Columbus
	Thomas M. Keegan	Helena
	Betty Wilkins	Missoula
	Donald J. Sterhan	Billings
Department of Administration	Scott Darkenwald, Director	
Montana Lottery	Jerry LaChere, Montana Lottery Director	
	L. John Onstad, Director of Security	
	Paul Gilbert, Information Systems Manager	

Executive Summary

State law requires the Legislative Audit Division conduct a comprehensive audit every two years of all aspects of security in the operation of the Montana Lottery. Our primary audit objective is to evaluate the existence and operation of security controls and evaluate compliance with state law.

To ensure our audit objective was met, we evaluated compliance with internal security policies and procedures and applicable federal tax withholding requirements and state law. We evaluated the existence and operation of security controls by obtaining documentation for compliance testing and review, interviewing Lottery management and staff, and observing daily operation activities. Automated audit tools were used to evaluate security over the network environment.

Included in our review is the implementation status of the four prior audit recommendations. All four recommendations have been implemented as they relate to:

- Completeness of required information on employment forms and retailer applications;
- On-line paper ticket stock storage and procedures for removing and adding ticket stock;
- Improving procedures for maintaining the non-player database; and
- User access rights to the Internal Control System and the Game Management System.

The current report contains nine recommendations addressing areas providing a more secure environment over Lottery security operations. The areas address:

1. Network access;
2. Network service accessibility;
3. Internet Information Server;
4. Anonymous user access;
5. Anonymous file transfer protocol;
6. Computer security;

7. Physical security;
8. Security investigations; and
9. Documentation.

Chapter I - Introduction and Background

Introduction

The Montana State Lottery (Lottery) was created in 1987 with the net revenue supporting the Teacher's Retirement Fund. In 1995, the legislature determined that all net profits from the sale of lottery tickets be transferred quarterly to the state's General Fund. The Lottery is funded from an enterprise fund with revenue derived primarily from participation in lottery games. In fiscal year 2003, the Lottery transferred $7.4 million to the General Fund.

A five-member State Lottery Commission, appointed by the Governor, oversees the Lottery's operations, sets policy, and determines the type and form of lottery games. The Lottery designs and markets lottery games that allow players to purchase chances to win a prize. The Lottery presently offers a variety of games, some in cooperation with other lotteries through the Multi-State Lottery Association (MUSL). Montana Cash is an on-line game offered exclusively to Montana players.

Instant Games

Instant games were the first games offered by the Lottery. Instant tickets are printed by Oberthur Gaming in San Antonio, Texas and shipped to the Helena Lottery headquarters. The Lottery inspects the shipment to ensure all tickets are present, play symbols are covered by latex, the latex covering is free from scratches, and the general appearance of the ticket is acceptable. The Lottery then distributes tickets to retailers, via UPS, for sale to the public.

The Lottery offers 40 different scratch games with varying top prizes and ticket costs ranging from one to five dollars. These games involve scratch tickets with particular themes. Players determine if they are winners by following directions on the individual game tickets and scratching the latex coating off the play area of a ticket to win the prizes tied to the ticket. Top prizes for these games range from less than $100 to tens of thousands of dollars. Prizes for winning tickets must be claimed within six months of the last day of sale. A state tax of 10 percent and a Federal tax of 25 percent are applied to all winnings over $5,000. Lottery retailers automatically validate winning instant tickets by scanning the bar code on the back of the ticket. Scratch ticket prizes of $250 or less can be claimed at

any Montana Lottery Retailer or at the Lottery headquarters in Helena. Prizes of more than $250 must be claimed at Lottery headquarters or by mailing a completed claim form and the signed ticket to the Lottery.

On-line Games

In addition to instant games, the Lottery offers players four on-line games. On-line games offer players a chance to win larger prizes than can typically be won on instant games.

- Powerball is offered in conjunction with 25 other lotteries. Jackpot sizes are based on sales; this cooperative effort offers smaller states like Montana the benefit of multi-million-dollar jackpots. The Powerball jackpot starts at $10 million and is an annuity with a cash option.
- Wild Card 2 is a game offered in Montana, Idaho, and South Dakota. The Wild Card 2 has a minimum cash jackpot of $100,000, combined with six other prize levels from $1 to $5,000.
- Hot Lotto is a game offered in Iowa, Minnesota, Montana, New Hampshire, South Dakota and West Virginia. Hot Lotto features a minimum $1 million growing annuity jackpot and eight other prize levels from $2 to $10,000.
- Montana Cash is the only on-line game specific to Montana. Montana Cash offers players a chance to win a guaranteed minimum cash jackpot of $20,000 and two other prize levels of $5 and $200.

On-line game prizes must be claimed within six months of the drawing. Retailers can validate and cash on-line game prizes of $599 or less. Prizes in excess of $599 must be claimed at the Lottery headquarters or by mailing a completed claim form and signed ticket to the Lottery.

Lottery Systems

The Lottery contracts with two vendors, Scientific Games International (SGI) and Oberthur Gaming. Oberthur Gaming is responsible for printing the scratch ticket games, and SGI is contracted to implement the instant and on-line games, and provide on-line ticket stock and hardware for gathering retailer sales data and validating winning tickets. SGI is headquartered in New York City,

with a satellite office in Helena. SGI subcontracts with eSuccess to provide the Internal Control System (ICS). The ICS independently verifies daily sales and validates winners for each game drawn.

SGI administers the Game Management System (GMS) for both on-line and instant games from a data processing center located in Helena. The system maintains retailer's sales data, the scratch ticket stock inventory, retailer data including licensing, phone contacts, retailer commissions from ticket sales, and validation of winners. SGI operates and maintains the electronic retailer network. The network connects over 592 terminals. The terminals are used to sell, print, and validate lottery tickets.

eSuccess administers and maintains the ICS. ICS is primarily used to independently verify winning tickets. ICS verifies sales and winners for each game drawn during the on-line game drawings.

Audit Objectives

State law requires the Legislative Audit Division to conduct a comprehensive audit every two years of all aspects of security in the operation of the Lottery. Our primary objective is to evaluate the existence and operation of security controls and evaluate compliance regarding the areas specifically enumerated in section 23-7-411, MCA:

a) Personnel security;
b) Lottery sales agent security;
c) Lottery contractor security;
d) Security of manufacturing operations of lottery contractors;
e) Security against ticket or chance counterfeiting and alteration and other means of fraudulently winning;
f) Security of drawings among entries or finalists;
g) Computer security;
h) Data communications security;
i) Database security;
j) Systems security;
k) Lottery premises and warehouse security;
l) Security in distribution;

m) Security involving validation and payment procedures;
n) Security involving unclaimed prizes;
o) Security aspects applicable to each particular lottery game;
p) Security of drawings in games whenever winners are determined by drawings;
q) The completeness of security against locating winners in lottery games with preprinted winners by persons involved in their productions, storage, distribution, administration, or sales; and
r) Any other aspects of security applicable to any particular lottery game and to the lottery and its operations.

Audit Scope and Methodology

The audit was conducted in accordance with Governmental Auditing Standards published by the United States General Accounting Office. We evaluated compliance with applicable federal tax withholding requirements and state law, state enterprise information technology policy, Lottery internal procedures, and MUSL security standards. We evaluated controls using criteria established by the National Institute of Standards and Technology (NIST), Microsoft Windows Server 2003 Security Guide, the Control Foundation's Control Objectives for Information and Technology (COBIT), and the computer security incident response team CERT® Coordination Center.

To ensure our primary objective was met, we reviewed retailer files to ensure compliance with state law and internal licensing procedures. "New hire" employee security files were reviewed for adherence to state law applicable to Lottery security and internal security investigation procedures. We evaluated whether security access to data is appropriate based on job responsibilities and whether processing logic accurately calculated tax withholding. We observed instant ticket stock distribution procedures and identified controls to deter ticket fraud. We evaluated physical security over the Lottery premises, warehouse and SGI contractor facilities. Automated audit tools were used to assess security strengths of the Lottery's Local Area Network (LAN), which consists of computers,

and associated devices that share a common communications line and typically share the resources of a single server.

Through document testing and review, observation of daily operations, and interview of key Lottery staff, we evaluated aspects of security controls in the operation of Lottery, including the implementation status of the four prior audit recommendations.

Prior Audit Recommendations

Our previous audit report (Montana Lottery Security, 01DP-07) contained four recommendations. Through interviews of key Lottery personnel, observation, and documentation review, we determined the Lottery implemented all four of the recommendations as they relate to:

- Completeness of required information on employment forms and retailer applications;
- On-line paper ticket stock storage and procedures for removing and adding ticket stock;
- Improving procedures for maintaining the non-player database; and
- User access rights to the ICS and the GMS.

Conclusion

Overall, the Lottery operates in compliance with federal tax withholding requirements. Security controls are in existence, but can be improved to ensure security of the Lottery operations and investigation procedures can be improved to ensure compliance with state law and internal procedures.

During the course of our audit, we identified an issue regarding employee investigation procedures, which we believe warrants management attention. This item is not included as a recommendation in this report but was discussed with the Lottery through an interim audit communication.

Chapter II - Network Security

Introduction

The Lottery maintains a Local Area Network (LAN) that consists of computers and associated office tools and equipment (hereafter called devices) that shares a common communications line and typically shares the resources of a single server. Inadequate network controls create the potential for a knowledgeable user to gain unauthorized or inappropriate access to the network where sensitive data is stored, and the administrators of the network do not intend unauthorized access. We utilized automated audit tools to test the security strengths of the network and its associated devices. We identified five areas where security over the network can be improved.

Network Access

MUSL standards specify that if the Lottery computer network is connected electronically to any third party computer networks other than the on-line system vendor, currently SGI, access controls must be in place to restrict or limit traffic between the two networks. The Lottery does not restrict user access to the Lottery network from the state intranet. The state intranet links agency networks allowing authorized members accessibility to share information and computing resources. Anyone with access to the state intranet can view computers on the Lottery's network and gather user account information on the computers. A knowledgeable user can use the account information to compromise the computer by gaining access to the data stored on the computer. While evaluating access controls, we viewed computers on the Lottery's network from the state intranet and gathered user account information. Because the Lottery is electronically connected to the state intranet, restricted access must be resident on the Lottery's network to limit traffic between the two sites to prevent a knowledgeable user from viewing data and directories on Lottery workstations, servers, and printers. Software exists to limit SGI traffic to the state intranet; however, there are no controls between the state intranet and the Lottery network to restrict access. According to Lottery personnel, they were unaware that traffic was not limited between the Lottery's network and the state intranet.

Chapter II - Network Security

Recommendation #1

We recommend Lottery comply with MUSL standards to ensure controls exist to restrict or limit access to network resources between the Lottery's network and the state intranet.

Network Service Accessibility

Printers and switches attached to the Lottery and SGI networks allow remote administration that is not password protected. Remote administration allows the changing of settings on a device for purposes of maintenance and configuration. The lack of password protection means that anyone can change settings on the printers and switches. Without password protection on remote administration a knowledgeable user could:

- Divert traffic to unauthorized locations on the network by modifying settings on the switch;
- Prevent printing on a printer by filling the print queue full of documents disrupting business continuity;
- Potentially disrupt network and/or print services through the modification of printer and/or switch settings disrupting management services and operations.

We identified seven printers on the Lottery's network allowing remote administration, which is not password protected.

GMS, administered by SGI, provides various services and information to the Lottery, such as retailer's sales data, retailer commissions from ticket sales, and validation of winners. Because of this relationship, SGI is an integral part of the Lottery's security control environment.

We identified three printers and two switches on SGI's network allowing remote administration that is not password protected. Switches essentially route data to an intended location. Changing a network switch setting could cause the failure of a network by preventing parts of the network from communicating with each other.

By default, remote administration is not password protected on printers and network switches. To protect these devices, it is necessary for the network administrator to manually set the password. Network staff at the Lottery and SGI were unaware of the need to password protect the remote administration to these devices or the potential risk they pose when unprotected.

Industry standards recommend identifying network services that are turned on by default and evaluate its necessity. The default configuration must then be modified to limit access and exposure, and the range of facilities and functions offered by the service to only those devices as necessary.

Recommendation #2

We recommend Lottery:

A. Password protect remote administration on printers; and

B. Require SGI to password protect remote administration on printers and switches.

Internet Information Server

A service known as Internet Information Server (IIS) is operating by default on seven SGI computers. IIS displays web pages to the intranet or Internet.

The Lottery connects to GMS through one of the machines, running the IIS web service, located at the SGI facility in Helena. The remaining six computers are operating IIS by default, not using IIS to provide web services. IIS based web sites have been susceptible to computer virus attacks and multiple viruses have been known to target IIS creating unexpected and undesirable events across networks. Upon identification of the default IIS service operating on these six machines, the SGI network administrator ran an IIS lockdown tool to protect IIS against potential attacks and viruses by deactivating unused parts of IIS that are most susceptible to attacks; however, the unused IIS service was not disabled. According to SGI

staff, IIS was not disabled because SGI staff did not realize the potential risks associated with IIS.

Industry standards recommend identifying any network service turned on by default and evaluating its necessity. The default configuration should be modified to limit access and exposure.

Recommendation #3

We recommend the Lottery require SGI evaluate the need and use of default IIS services and modify the default configuration to limit access and exposure.

Anonymous User Access

In order to facilitate the communication of computers in a network environment, the operating system used by the Lottery has a built-in function that allows anonymous connections by default. An anonymous connection is where one computer can connect to another without providing the username/password, or the authentication credentials. This anonymous connection does not directly allow access to data stored on the computer; however, it does allow a knowledgeable user to gain a complete listing of all user accounts that have ever logged onto a specific computer and use this knowledge to access data stored on the computer. We identified 15 computers on the Lottery's network that are operating at the default level, allowing any machine anonymous access. Two higher levels of security are available. Level one restricts access to user account information, and Level two denies anonymous connections requiring all computers to provide credentials. The default setting has not been changed because Lottery personnel were not aware of the low level of protection defined by the default setting. Industry standards recommend using the configuration principle "deny first, then allow" and configure the service to allow only authenticated connections.

Recommendation #4

We recommend the Lottery evaluate the risk of the default setting that allows anonymous connections between computers and implement higher levels of security as needed.

Introduction

File Transfer Protocol (FTP) is a computer protocol that facilitates the storing and transfer of files on a server, primarily as a public service. Anonymous FTP is an implementation of this service that allows access to file sharing and storage without user authentication by providing a username or password.

Anonymous File Transfer Protocol

The Lottery uses anonymous FTP, enabling any user to log into the FTP server without providing an authentic username or password. Users can access anonymous FTP services by using "Anonymous" as the username and any e-mail address as the password. We identified one computer on the Lottery's network that uses this service to enable the subcontractor, eSuccess, to update the ICS computer. We further identified four SGI computers operating this service for the purpose of downloading software for routers. Anonymous FTP is most commonly used where public access to files is a priority and is not appropriate for use in circumstances where files are not intended to be shared publicly. Anonymous FTP, as used by the Lottery and SGI, is not necessary and the services provided by anonymous FTP can be achieved by requiring user authorization in order to secure FTP services. According to Lottery and SGI personnel, anonymous FTP has not been disabled since neither Lottery nor SGI personnel realized the potential risk involved with this service. Industry standard recommends configuring the service to allow only authenticated connections.

Recommendation #5

We recommend the Lottery evaluate the risk of anonymous FTP service and ensure FTP services require user accountability.

Chapter III - Computer Security

Introduction

Computer security is facilitated by granting users specific or defined rights and permissions, through user accounts having a direct relationship to files and directories.

Computer Security

The Lottery's operating system has built-in user accounts with default names that cannot be deleted, but can be renamed. A common built-in account is "Administrator." An administrator account is a type of user account that grants full control over a computer and allows full access to all data and resources on a computer. While evaluating computer security, we identified two issues pertaining to administrative accounts:

- the use of the well-known default username "Administrator," and
- the existence of multiple administrator accounts on workstations.

We identified 15 workstations each having at least four administrator accounts; some having up to seven. The Lottery uses one of these accounts for update and management of computers. The username on this account is "Administrator" and according to Lottery personnel the password is only updated when there is turnover among the information technology staff. Lottery personnel have not prioritized modifying the default username, since they did not view this as a measurable risk that could adversely compromise the system. According to industry standards, the administrator account should be renamed from the default name "Administrator" to prevent knowledgeable users from using the well-known account name to gain access to a computer and/or network. Also, state enterprise policy requires passwords to be changed at least every 60 days. Unchanged passwords increase the risk that systems may be compromised.

The remaining administrator accounts not used for update, were renamed and assigned to Lottery personnel using the computer during employment. According to Lottery personnel, the multiple accounts on each of the 15 workstations were the result of old administrator accounts not being removed when personnel transitioned or network staff changed. In addition, each machine has

the default administrator account plus an administrative account for each of the three members of the information technology staff. Lottery personnel stated that administrator accounts are needed to access software, such as picture scanning software used in the graphic design of Lottery scratch tickets. However, a multiple number of administrator accounts increases the risk for a knowledgeable user to compromise one of the accounts and gain administrator access to a computer and/or the network. A user with administrator access rights has full control over the computer and complete access to all data and resources on the computer.

Recommendation #6

We recommend the Lottery:

A. Change the administrator account default username, and change the password on the administrator account in accordance with state policy; and

B. Eliminate unused administrator accounts.

Chapter IV - General Security

Introduction

A security control review provides information about the security environment in which Lottery operates. State law requires the Lottery to maintain a high degree of security over its operation and games. The following three sections discuss areas where Lottery can enhance compliance with state policy and internal procedures.

Physical Security

SGI owns and operates a warehouse in the Helena area that provides physical storage of on-line ticket stock and Lottery hardware, such as retailer terminals. We performed a walk-through of SGI premises and identified an unsecured door located on the outside of the facility. The door leads to the attic and is held closed by a latch and a bent piece of wire. Through this door, an individual could potentially gain access to the warehouse and circumvent established physical security controls. Industry standard recommends restricting physical access to authorized individuals. SGI and Lottery personnel stated they were not aware of the existence of the door leading to the attic.

Recommendation #7

We recommend the Lottery require SGI secure the attic door to deter unauthorized physical access to the warehouse facility.

Security Investigations

The Lottery has established procedures and forms to assist with ensuring security over its operations. Security investigations are performed for new hires, retailers, and owners and employees of contractor/vendors. Prior to issuing a retailer sales agent license, Lottery evaluates retailer applicants to determine their eligibility to become a Lottery game retailer. Contractor/vendors seeking to provide goods and services to Lottery are evaluated to determine their suitability.

Contractor/Vendor Investigations

The Lottery has established internal vendor and contractor investigation procedures requiring a credit and criminal history inquiry. Credit and criminal history inquiries will be performed on those contractor and vendor owners seeking to provide services to the Lottery and those who will provide direct service to the Lottery.

The corporate filings of the business seeking the contract will be examined to determine listed ownership and parties of interest.

Documentation on required credit history and/or felony checks did not exist for owners of the external accounting firm and owners of the janitorial services company. According to Lottery personnel, the credit history and felony checks were performed; however, documentation could not be provided to substantiate the existence of the inquiries.

Retailer Investigations

Prior to issuing a new retailer lottery sales agent license, state law requires the Lottery consider the financial responsibility and security of the applicant and the applicant's business or activity. The Lottery has established internal retailer application licensing procedures requiring a criminal background search and credit history inquiry for all individuals possessing 10% or more ownership in the business applying for a new lottery license. Lottery tickets or chances may be sold only by licensed sales agents.

We sampled 27 files of new retailers licensed from May 2001 to June 2003. From our sample, we reviewed the files of three parent companies and 27 retailers to ensure the required credit history and/or felony checks were performed. Our sample testing indicates that while past credit and/or criminal inquiries exist, the documentation dates back to 1987 for some files. The Lottery's current practice is to carry forward the inquiries in cases where retailers are applying for an additional license.

The Lottery is in the process of developing a formal policy to establish a timeframe for a definition of "current" for credit history and criminal investigations documentation. Since "current" has not been defined, policy has not been enforced to ensure the existence of current documentation; rather, past credit history and/or felony checks are carried forward.

Recommendation #8

We recommend the Lottery:

A. Ensure credit and criminal inquiries are performed and documentation exists for owners of the external accounting firm and owners of the janitorial services company; and

B. Define in policy, a definition of "current" for the aging of credit history and criminal investigation documentation.

Documentation

The Lottery does not have a documented:

- Network security plan;
- Backup archival procedures;
- Complete disaster recovery plan; or
- System and software change procedures.

Section 2-15-114, MCA, requires each department head to ensure an adequate level of security for all data and information technology resources within that department and shall develop and maintain written internal policies and procedures to ensure security of data and information technology resources. State policy states that each agency must have a written backup plan including a backup schedule, backup process and a list of mission critical applications. The backup process cannot be used as an electronic archiving method and a separate electronic archiving process and plan must be developed.

The Lottery has taken steps to formalize documentation by completing a partial disaster recovery plan. Other plans and procedures are informal and are not documented or established. As discussed in recommendations 2, 3, and 4, network settings and services maintain default settings, increasing the risk that a knowledgeable user may compromise the system. Formalized operational practices and procedures enhance system awareness to reduce security lapses and oversight. For example, during the audit we identified an entry in a routing table located on the Lottery network, which Lottery personnel were unable to explain or describe

its purpose. Documentation did not exist to explain this entry, nor were the Lottery personnel able to disclose a purpose. The Lottery later determined this entry allows the ICS machines, which are not located on the Lottery network, to print to the Lottery network. According to Lottery personnel, the prior network administrator did not maintain documentation. The current network administrator is developing documentation.

Documentation of all aspects of computer support and operations promotes continuity and consistency of business operations. Establishing and formalizing operational practices and procedures with sufficient detail helps provide a quality assurance function that will promote efficiencies and ensure operations are performed correctly, reduce security lapses and oversights, and gives new personnel sufficiently detailed instructions.

Recommendation #9

We recommend Lottery:

A. Document and implement a network security plan and complete and adopt the disaster recovery plan; and

B. Establish, document, and implement a backup archival procedure and software change procedures.

Montana Lottery Response

Montana Lottery

RECEIVED
SEP 2 6 2003
LEGISLATIVE AUDIT DIV.

September 24, 2003

Ms. Tori Hunthausen
Information Systems Audit Deputy
Legislative Audit Division
State Capitol Building
Helena, MT 59620-1705

Dear Ms. Hunthausen,

Thank you for the opportunity to respond to the report on Montana Lottery Security.

The Montana Lottery agrees with the audit findings and recommendations. We will take the necessary action to comply with all recommendations. Through the audit process, we will strengthen and improve the security of the Montana Lottery operation.

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

RECOMMENDATION #1

We recommend Lottery comply with MUSL standards to ensure controls exist to restrict or limit access to network resources between the Lottery's network and the state Internet.

We concur with the recommendation. We are not in violation of MUSL standards but we will install additional firewalls to comply with your recommendation by February 1, 2004.

RECOMMENDATION #2

We recommend Lottery:

A. Password protect remote administration on printers; and

B. Require SGI to password protect remote administration on printers and switches.

2525 North Montana Avenue • Helena MT 59601-0598
Phone 406-444-LUCK (5825) • Fax 406-444-5830

We concur with this recommendation. The Lottery has completed password protection on our printers. SGI has also protected their printers with passwords and is in the process of protecting switches. That work will be complete no later than November 1, 2003.

RECOMMENDATION #3

We recommend the Lottery require SGI evaluate the need and use of default IIS services and modify the default configuration to limit access and exposure.

We concur with your recommendation. SGI will evaluate the need and modify, as needed the default IIS services to limit access. This work will be completed by December 1, 2003.

RECOMMENDATION #4

We recommend the Lottery evaluate the risk of the default setting that allows anonymous connections between computers and implement higher levels of security as needed.

We concur with this recommendation. Work has been completed on all computers by setting the security level to a two.

RECOMMENDATION #5

We recommend the Lottery evaluate the risk of anonymous FTP service and ensure FTP services require user accountability.

We concur with the recommendation. This work has been completed by requiring both a username and a password.

RECOMMENDATION #6

We recommend the Lottery:

A. **Change the administrator account default username, and change the password on the administrator account in accordance with state policy; and**

B. **Eliminate unused administrator accounts.**

We concur with the recommendation. All work on this recommendation has been completed and complies with state policy. All unused administrator accounts have been deleted.

RECOMMENDATION #7

We recommend the Lottery require SGI secure the attic door to deter unauthorized physical access to the warehouse facility.

We concur with your recommendation. Scientific Games secured the attic door in question with appropriate locks on the day that the auditors visited the SGI facility.

RECOMMENDATION #8

We recommend the Lottery:

A. Endure credit and criminal inquiries are performed and documentation exists for owners of external accounting firm and owners of the janitorial service company; and

B. Define in policy, a definition of "current" for the aging of credit history and criminal investigation documentation.

We concur with your recommendation. The missing documentation for our janitorial service and external accounting firm have been redone and placed in appropriate files. We will define, in policy, an appropriate means of making current, retailer credit histories and criminal investigation documentation. Our policy will be written and in use by December 1, 2003.

RECOMMENDATION #9

We recommend Lottery:

A. Document and implement a network security plan and complete and adopt the disaster recovery plan; and

B. Establish, document, and implement a backup archival procedure and software change procedure

We concur with your recommendation. We will complete and implement a network security plan and our disaster recovery plan. We will document our backup archival procedure and system software change procedure. This work will be completed by March 31, 2004.

Thank you again for the opportunity to respond. We greatly appreciate the constructive and professional manner in which this audit was conducted. If you have questions regarding any of our comments, please do not hesitate to contact me.

Respectfully submitted,

L. John Onstad
Director of Security

Cc. Gerald J. LaChere, Director