TECHNICAL STANDARDS

FOR

ELECTRONIC RAFFLE SYSTEMS

LGA

Liquor and Gaming
Authority of Manitoba

800 - 215 GARRY STREET
WINNIPEG, MANITOBA R3C 3P3

Table of Contents

1 Overview of Technical Standards Document (TSD)

1.1 Introduction

1.1.1 General Statements I

The General Statements are as follows:

a) Before being permitted to operate, all gaming supplies used in the Province of Manitoba must be presented to the Liquor and Gaming Authority of Manitoba (LGA). The LGA will determine if these supplies should be tested to applicable requirements set forth in this Technical Standards Document (TSD) and if approval is required.

b) This TSD may apply in parts or in whole to a system proposed for use in the conduct of a raffle. The LGA will determine the applicable part/s to be met by a system and notify applicants or gaming suppliers of the required testing to be done.

c) For the purposes of this TSD, an Electronic Raffle System (ERS) shall be considered a gaming supply as defined in Section 4(e) of the Gaming Regulations.

d) An applicant or gaming supplier may select an Accredited Testing Facility (ATF), or other equivalent body, that has been licensed with the LGA, to perform required testing.

e) The appointed testing body must provide their final evaluation results, reports, and any additional documentation as may be required directly to LGA for review, and where required, subsequent discussion.

f) The LGA may accept internal quality assurance testing on an Electronic Raffle System; however, reliance on the test results for the purposes of approval is at the discretion of the LGA.

g) Any ATF or other equivalent body that is employed to perform testing, and is licensed by the LGA, must treat the applicant or gaming supplier as its client, and the LGA as the regulatory authority for issuing approvals. Although the appointed testing body may recommend the approval of any gaming supplies for use in the Province of Manitoba, the ultimate authority to approve gaming supplies rests solely with the LGA.

h) Any third-party service providers contracted to provide service involving accessing, processing, communicating or managing the sale of tickets through the Internet must adhere to information contained in this document. The security roles and responsibilities of third party service providers should be defined and documented as it relates to the security of information.

   i. Agreements with third party service providers involving accessing, processing, communicating or managing the purchase of on-line tickets through the Internet or its components, or adding products or services to the system used or its components, shall cover all relevant security requirements.

   ii. The services, reports and records provided by the third party shall be monitored and reviewed by LGA upon request.

   iii. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

   iv. The access rights of third party service providers to the system and/or its components shall be removed upon termination of their contract or agreement, or adjusted upon change.

1.1.2 General Statement II

The LGA reserves the right to modify (or selectively apply) the requirements set forth in this TSD as deemed necessary to ensure the integrity of gaming in the Province of Manitoba. In order to ensure consistency and compliance, the LGA commits to providing reasonable written notice to any licensee or gaming supplier, on an as-needed and case-by-case basis.

1.2 Manuals

Operation manuals and service manuals must be expressed in broad terms that are directly relevant to the system used to sell raffle ticket(s) and must be provided at the request of LGA.

a) Operational manuals associated with the applicable system.

b) Technical Service manuals which:

   i. Accurately depict the system for which the manual is intended to cover;

   ii. Provide adequate detail and be clear in their wording and diagrams to support interpretation by LGA personnel;

   iii. Include a maintenance schedule outlining the elements of the system that require maintenance and the frequency at which that maintenance should be carried out;

   iv. Include a maintenance checklist that enable appropriate staff to make a record of the work performed and the results of the inspection; and

   v. Include a complete list and samples of available reports that can be generated by the system.

c) Technical documentation that must provide adequate detail and be sufficiently clear in wording and diagrams to enable the review /evaluation of the system used.

d) Complete documentation for programming patches, fixes and any upgrades made to the system.

1.3 Acknowledgment of Other TSDs Reviewed

1.3.1 General Statement

This TSD has been developed by reviewing and using portions of the documents listed below:

a) Gaming Laboratories International Standard (GLI-31) - Standards for Electronic Raffle Systems (ERS).

b) Gaming Policy and Enforcement Branch (GPEB) - Technical Gaming Standards for Electronic Raffle Systems (TGS6) and for Internet Gaming Systems (TGS5).

c) Saskatchewan Liquor and Gaming Authority - Standards for On-line Raffle Ticket Sales.

1.4 Purpose of TSD

1.4.1 Purpose

The Purpose of this TSD is as follows:

a) To eliminate subjective criteria in analyzing and certifying Electronic Raffle Systems operation.

b) To only test those criteria which impact the credibility and integrity of Electronic Raffle Systems operation from both the Revenue Collection and Player’s game play point of view.

c) To create a TSD that will help ensure that Electronic Raffle Systems operating in the live environment are fair, honest, secure, safe, auditable, and able to operate correctly.

d) To recognize that Testing which does not impact the credibility and integrity of the Electronic Raffle System (such as Electrical Testing) should not be incorporated into this TSD but left to appropriate test laboratories that specialize in that type of testing.

e) To recognize that except where specifically identified in this TSD, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer of the equipment.

f) To construct a TSD that can be easily changed or modified to allow for new technology or functionality.

g) To construct a TSD that does not specify any particular method or technology for any element or component of an Electronic Raffle Systems. The intent is instead to allow a wide range of methods and technologies to be used to comply with this TSD, while at the same time, to encourage new methods and technologies to be developed.

1.4.2 No Limitation of Technology

One should be cautioned that this TSD should not be read in such a way that limits the use of future technology. The TSD should not be interpreted that if the technology is not mentioned, then it is not allowed. As new technologies are developed, the LGA, will review this TSD, make any changes deemed necessary, and incorporate new minimum standards for the new technology.

1.5 Other Documents That May Apply

1.5.1 Other TSDs

This TSD, as well as the other TSDs listed below, are to be interpreted so that all of the provisions are given as full effect as possible. In the event of a conflict or inconsistency between the foregoing, unless expressly stated to the contrary, the order of precedence shall be as follows:

a) This TSD

b) GLI 31 - Electronic Raffle System

c) GLI 13 - On-line Monitoring and Control Systems v2.2.

d) GLI 21 - Client-Server Systems v2.2

e) GLI 27 - Network Security Best Practices v1.1

1.5.2 Legislated Acts or Regulations

The following legislations take precedents over this TSD:

a) The Criminal Code of Canada

b) The Liquor and Gaming Control Act and Gaming Regulation, of Manitoba

c) The Manitoba Freedom of Information and Protection of Privacy Act

1.5.3 Information Systems Security (ISS) Industry Standards

The Administrative Controls, Technical Controls and Physical & Environment Controls for the Electronic Raffle Systems should incorporate the best practice principles found in the applicable and relevant ISS industry standards, as dictated by such sources as:

a) ISO / IEC 27001 – Information Security Management Systems (ISMS);

b) ISO / IEC 27002 – Code of practice for information security management;

c) ISO 31000:2009 – Risk Management – Principles and guidelines;

d) Control Objectives for Information and Related Technology (COBIT); and

e) Open Source Security Testing Methodology Manual (OSSTMM).

1.6 Definitions

i. **Access control** – the restriction of access to a place or other resource. Locks and login credentials are two mechanisms of access control.

ii. **Accredited Testing Facility (ATF)** – a test facility or laboratory licensed by the LGA for the purpose of gaming supply testing.

iii. **Address Resolution Protocol** (**ARP**) – the protocol used to translate IP addresses into MAC addresses to support communication on a LAN (Local Area Network).

iv. **Algorithm** – a finite set of unambiguous instructions performed in a prescribed sequence (mathematical rule or procedure) used to compute a desired result.

v. **Authentication** – a security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message or originator.

vi. **Bi-Directional** – the ability to move, transfer or transmit data in both directions.

vii. **Crypto-analytic** – an attack against the encryption key (refer to definition of encryption key).

viii. **Cryptographic** – anything written in a secret code, cipher, or the like.

ix. **Distributed Denial of Service (DDoS)** – a type of DoS attack where multiple compromised systems are used to target a single system causing temporary interruption or suspension of the services of a host.

x. **Domain** – a group of computers and devices on a network that are administered as a unit with common rules and procedures.

xi. **Draw Number** – a uniquely identifiable number that is provided to the purchaser for each chance purchased and is eligible to be selected as the winning number for the raffle.

xii. **Electronic Raffle System (ERS)** – means computer software and related equipment used by raffle licensees to sell tickets, account for sales, determine winners through random selection, and/or for the disbursement of prizes.

xiii. **Encryption** – the reversible transformation of data from the original (plaintext) to a difficult-to-interpret format (ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity.

xiv. **Encryption Key** – a sequence of characters used to encrypt or decrypt data.

xv. **Entry** – a physical (counterfoil) or electronic record which will be used to determine a winner, and contains a single draw number matching the purchaser's ticket, and may, depending on the type of raffle, contain the name, address, or telephone number of the purchaser.

xvi. **Firewall** – any number of security schemes that prevent unauthorized communication to and from a network.

xvii. **Geolocation** – refers to identifying the real-world geographic location of an Internet connected computer, mobile device, or website visitor.

xviii. **Host** – a computer or other device connected to a network that offers information, services or applications to the network.

xix. **Hypertext Transfer Protocol (HTTP)** – the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

xx. **Internet** – an interconnected system of networks that connects computers around the world via the TCP/IP protocol.

xxi. **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)** – the process of monitoring computer and network activities, and analyzing those events to look for signs of intrusion in the system.

xxii. **IP Address** – short for Internet Protocol address and is an identifier for a computer or device on a TCP/IP network.

xxiii. **MAC Address** – short for Media Access Control address is a hexadecimal sequence, embedded in all communication hardware, which can uniquely identify any device on a network.

xxiv. **Man-in-the-Middle (MITM)** – an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.

xxv. **Message Authentication** – a short piece of imbedded code used to prove the integrity and authenticity of a transmission packet.

xxvi. **On-line** – refers to being connected to the Internet.

xxvii. **On-line Platform** – refers to the ERS hardware and software which drives the features common to all raffles offered, and which forms the primary interface to the Raffle System for both the patron and the operator.

xxviii. **Price Points** – tickets sold in groups containing a specific quantity of draw numbers at a discounted price (e.g. 3 for $10, 10 for $20, etc.).

xxix. **Protocol (Communication)** – a set of formal rules describing how to exchange data across a network.

xxx. **Raffle Sales Unit (RSU)** – an RSU may be a portable/wireless device, a remote hard-wired connected device or a standalone cashier station that is used as a point of sale for tickets.

xxxi. **RFC 1918** – standards related to the use of Internet addressing, private IP address space and the use in a private network.

xxxii. **Security Certificate** – information often stored as a text file and is used by the SSL (Secure Socket Layers) Protocol to establish a secure connection; both sides must have a valid Security Certificate, which is also called a Digital ID.

xxxiii. **Seeding/Re-Seeding** – the method of determining the initiating value (seed) to be used by the RNG algorithm.

xxxiv. **Server** – a running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which "servers" are computer programs running to serve the requests of other programs (clients).

xxxv. **Shellcode** – a small piece of code used as the payload (cargo of data transmission) in the exploitation of computer security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a computer system's information assurance.

xxxvi. **Stateless Protocol** – a communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

xxxvii. **TCP/IP protocol** – Transmission Control Protocol/Internet Protocol which is the suite of communications protocols used to connect hosts on the Internet.

xxxviii. **Ticket** – means the physical or electronic record provided to a purchaser as confirmation of participation in a draw.

xxxix. **Validation Number** – means a unique number which may represent one or more draw numbers that will be used to validate the winning number for the raffle. A validation number must also include a barcode.

xl. **Website** – or simply site, is a set of related web pages typically served from a single web domain.

xli. **World Wide Web** – or simply the Web, is a hypertext system that operates over the Internet.

1.7 Phases of Testing

1.7.1 General Statement

The LGA will determine if an ERS is to be certified in one or two phases:

a) Initial ATF testing, where the ATF will test the integrity of the system in conjunction with supplied Raffle Sales Units, in a laboratory setting with the equipment assembled; and

b) On-site testing following the initial install of the system to ensure proper configuration of the security applications. This may include, but is not limited to conducting event simulations with and without challenges to system operations, testing the stability of the system at maximum anticipated loads, verifying the internal controls and IT infrastructure, and any other tests as mandated by the LGA.

2 Raffle Management Requirements

2.1 General Operating Procedures

2.1.1 General Statement

An Electronic Raffle System (ERS) will have one or all of the following:

a) Raffle Sales Units (RSU’s) or other electronic means (on-line) that provide for the sale of tickets.

b) The ability to support all RSU's whether they are hard-wired or connected wirelessly to ensure that each unit sends or transmits all ticket sales to the system.

c) Equipment or software necessary for the collection, tracking, and accounting of all transactions initiated through the raffle system.

d) A Random Number Generator (RNG) program that will randomly select entries in a draw.

e) In the event of a manual draw process, a solution that facilitates the printing and collection of entries into a draw drum and ensures that each entry has an equal chance to be drawn.

f) Equipment or software that provide for the disbursement of prizes.

2.1.2 Licence Compliance

An ERS must operate in a manner that fully complies with the licence conditions and rules of play under which the licence has been issued.

2.1.3 Prize and Sales Limitations

An ERS must be capable of configuring limits for the maximum amount that may be won and the maximum number of tickets to be sold. These settings must be implementable if required by the licence conditions.

2.1.4 Time Limits

An ERS must be capable of providing a configurable time limit that can be set to:

a) Close sales

b) Terminate the draw

2.1.5 System Configuration Changes

The ERS must ensure that configuration settings cannot be modified without an authorized secure logon.

2.1.6 Account Registration

The ERS or an associated on-line platform must employ a mechanism (either online or via a manual procedure approved by the LGA) to securely collect information required to complete registration of a purchaser account. Once the identity verification is completed, and the purchaser has acknowledged all of the necessary privacy policies and the terms and conditions, the purchaser account can become active. The purchaser must be fully registered and their account must be activated prior to permitting ticket purchases.

2.1.7 Geolocation

The Raffle System, Online Purchasing Platform and/or the Patron Device must be able to reasonably detect the physical location of an authorized patron attempting to access the service. Third parties may be used to verify the location of patrons as allowed by the LGA.

2.2 Tickets and Entries

2.2.1 General Statement

a) An ERS must be capable of generating, and printing through RSU or distribute on-line, a ticket with one or more uniquely identifiable draw numbers.

b) The system must not generate duplicate draw numbers within the same event.

c) For each draw number generated, there must be one and only one matching entry with the same draw number.

d) The ERS must only generate tickets and entries for the current event.

e) The ERS must not generate additional entries for ticket reprints.

2.2.2 Tickets

A purchaser shall receive a ticket as a transaction record for one or more chances to win in a raffle draw. A ticket must be issued with the following information at a minimum:

2.2.2.A General Raffles

i. Name and address of the licensee

ii. Location, date and time of respective draw/s

iii. Description and value of the prize/s

iv. The order in which the prizes will be awarded. Applicable for draw with multiple prizes

v. One or more unique draw numbers generated by the ERS

vi. Number of tickets available for sale

vii. Price of the ticket

viii. The LGA licence number to be displayed as LGA___RF

ix. any restrictions that may be placed on awarding prize/s

x. An indication that every ticket holder has the right to witness the draw/s

xi. Issued date and time in 24 hour format showing hours and minutes

xii. Unique validation number or barcode

2.2.2.B 50/50 Raffles

i. Name and address of the licensee

ii. Event Identifier

iii. The LGA licence number to be displayed as LGA___RF

iv. One or more unique draw numbers generated by the ERS

v. Issued date and time in 24 hour format showing hours and minutes

vi. Price of the ticket

vii. Statement of where and when draw will be held

viii. Statement that winner must have ticket to claim prize and number of days in which to claim (for tickets where purchaser’s information is not required); and any other restrictions that may be placed on awarding prize/s

ix. Unique Validation number or barcode

x. The words “keep ticket until winner is confirmed”

Note: *Where a series of raffles is conducted under a single licence, tickets for each raffle must be differentiated from the other tickets used in the series (i.e. unique ticket numbers). If a series of draws are conducted on a single day, the tickets sold for each draw must be uniquely identifiable from tickets sold for other draws conducted on the same day (i.e. different event identifier).*

2.2.3 Entries

All entries used in a raffle drawing must either be printed or entered electronically for each purchased draw number. Printed entries must be the same size, shape, and weight. All entries must have an equal chance of being selected. The system must generate a unique entry for each draw number sold on a ticket. An entry must be printed or entered electronically with the following information, at a minimum:

2.2.3.A General Raffles

i. The name, address and telephone number of the ticket purchaser

ii. One draw number which exactly matches a single draw numbers from the ticket issued to the purchaser

iii. Event Identifier

iv. Processed date and time in 24 hour format showing hours and minutes

v. Unique validation number or barcode

2.2.3.B 50/50 Raffles

i. The name, address and telephone number of the ticket purchaser (multi-days 50/50 only)

ii. One draw number which exactly matches a single draw numbers from the ticket issued to the purchaser

iii. Event Identifier

iv. Processed date and time in 24 hour format showing hours and minutes

v. RSU identifier from which the entry was processed

vi. Price of associated ticket

vii. Unique Validation number or barcode

Note: *Where the requirements above become cumbersome for use in a Random Number Generator database or poses printing problems, an alternative will be considered provided that the information for each entry is securely recorded elsewhere and can be easily traced directly to the respective alternative.*

2.2.4 Additional Printed Information

It is permissible that a ticket may contain additional printed information, i.e. advertising, logos, coupons, etc. Some of this information may be contained on the ticket stock itself. Any additional printed information must not impact or obscure the required printed information as noted in sections 2.2.2.A/B of this standard.

2.2.5 Validation Numbers

The algorithm or method used by the ERS to generate the ticket validation number must be unpredictable and must ensure that there is no duplication of validation numbers for the raffle currently in progress.

2.2.6 Voiding a Ticket

The ERS must be capable of voiding a ticket after a sale has been completed.

a) If a ticket is voided, the appropriate information which includes the draw number(s) and the validation number(s) pertaining to the voided ticket shall be recorded in the ERS.

b) Voided draw numbers shall not be available for resale or re-issue.

c) The ERS must flag or otherwise identify in the system, a voided ticket and its corresponding draw number(s) in support of the winning number validation process.

d) The ERS must automatically adjust the total sales figure when a ticket is voided.

2.3 Raffle Prize Display

2.3.1 Active Jackpot Display (50/50)

An ERS that supports a display of the current jackpot that is intended to be viewed by purchasers of the raffle, that display shall indicate the raffle prize to be half the amount of gross sales in Canadian Dollars and represents the current progression of the prize. If the display is gross sales it should be followed by a message indicating that the winner gets half.

***Note**: It is accepted that, depending on the medium and system configuration, communication delays may prevent an accurate reconciliation between the displayed prize jackpot and the system prize jackpot at any given point during the event.*

2.3.2 Winning Draw Number Display

An ERS that supports a display of the winning draw number at the location of the event shall display the winning draw number in the same format as was entered into the draw and shall display the number on all capable display devices that are intended to be viewed by purchasers.

2.4 Closing Sales

2.4.1 General Statement

The ERS must have the ability to set time limits for which tickets may be purchased and limits for the number of tickets available for sale. Upon expiration of the purchase period and/or completion of sale of the final ticket, the ERS must be capable of closing sales automatically.

2.4.2 Time and Ticket Closure

The time of the sales closing may be:

a) Configurable within the ERS, or

b) Manually enabled by the Licensee.

2.4.3 Sales Closure

The ERS must be capable of notifying that all sales from RSU devices and/or on-line have been uploaded, transferred or otherwise communicated to the server, upon closure of sales.

a) On verification of the sales data transfer, RSU devices must be capable of being reset.

b) The RSU and/or on-line platform must be incapable of ticket sales for the current raffle.

2.4.4 Time and Ticket Counter Display

The ERS must be capable of displaying by way of the RSU and/or on-line the time and/or the amount of tickets remaining for sales to be closed. The sales closure, when it occurs, must also be displayed.

2.4.5 Reconciliation

The ERS must be capable of reconciling all sales including sold, unsold and voided sales for the raffle purchase period to ensure that only valid draw numbers are eligible to win.

2.5 Winner Determination

2.5.1 General Statement

The licensee will conduct a draw in accordance with the rules and standard procedures as stipulated in their license.

2.5.2 Drawn Number Validation

On completion of the draw, the ERS must have the facility to verify the status of the draw number (i.e. valid draw number or voided draw number).

2.5.3 Winner Verification

a) The ERS must be capable of verifying the winning ticket presented by the purchaser to the licensee either manually, or if applicable, through the use of a bar code scanning device reading the validation number.

b) After verification, the ERS must record and retain the winning number within the system database.

2.6 Accounting Reports

2.6.1 General Statement

The ERS must be capable of producing general accounting and exception reports.

2.6.2 Standard Event Reporting

The following data will be required to be maintained for each raffle drawing:

a) Date and time of Event

b) Licensee Identification

c) Sales information (Sales totals, refunds, voids, reprints and sales by price point)

d) Prize distribution

   i. Prize award to winning participant
   ii. Revenue retained by Licensee (for 50/50 raffle)

e) Refund totals by event

f) Draw numbers-in-play count

g) Winning number drawn

h) Other reports required by the LGA

2.6.3 Accounting Reports

All activities on the reports must be date and time stamped, and the reports sortable by any field. The ERS must, at a minimum provide the following reports:

a) Error/Exception Report –Exception information including, but not limited to, changes to the raffle configuration, corrections, overrides, reprints (tickets and entries) and voids.

b) Ticket Report – A report which includes a list of all ticket sold including all associated draw numbers and selling price points.

c) Sales by RSU – A report which includes a breakdown of each RSU's total sales, including draw numbers dispensed and any voided or misprinted tickets or reprint requests.

d) Sales on-line – A report which includes a breakdown of on-line sales, including draw numbers issued and any voided or faulty tickets or reissue requests.

e) Sales Summary by Price Point – A report that summarizes the number of tickets sold at a particular price point and expresses the total dollar value of the sales for each. The summary should also provide an aggregate total for this information.

f) Voided Draw Number Report – A report which includes a list of all draw numbers that have been voided including corresponding validation numbers.

g) RSU Event Log - A report which lists all events recorded for each RSU, including the date & time, a brief text description of the event and/or identifying code.

h) On-line Event Log - A report which lists all events recorded for on-line sale of tickets, including the date & time, a brief text description of each event and/or identifying code.

i) RSU Corruption Log – A report which lists all RSUs that are unable to be reconciled to the system, including the RSU identifier, RSU operator, and the money collected.

j) On-line Corruption Log. A report which lists all on-line transactions that were unable to be reconciled to the system.

3 Raffle Sales Unit (RSU) Requirements

3.1 Introduction

3.1.1 General Statement

a) An RSU is comprised of a combination of hardware and software configured to operate as a point of sale that will print tickets as described in sections 2.2.2.A/B of this standard.

b) Tickets may be purchased from an attendant-operated or a player-operated RSU. Any other methods will be reviewed and approved by LGA on a case-by-case basis.

3.2 Raffle Sales Unit Types

3.2.1 Attendant-operated RSU

a) Tickets may be sold by an attendant. Upon receiving payment for the ticket, the attendant will cause the RSU to print a ticket with the corresponding draw numbers based on the purchaser's request and the pricing model for the raffle.

b) It is permitted that the attendant-operated RSU may be configured as a mobile/wireless option or as a fixed connection option.

3.2.2 Player-Operated RSU

a) Tickets may be sold through a stand-alone sales unit that has been correctly configured for the current raffle. A participant can make a purchase following the instructions appearing on the screen of the player-operated RSU. Upon verification of payment, the RSU will print or dispense or cause to be delivered a ticket with the corresponding draw numbers to the purchaser based on the purchaser’s request and the pricing model for the raffle.

b) A player-operated RSU must be configured with a fixed connection option.

3.3 Raffle Sales Unit Operations and Security

3.3.1 Access Controls

a) Access to raffle sales software shall be controlled by a secure logon procedure. It is recommended that the software have the ability to automatically lock up or logoff after a configurable amount of inactivity.

b) An RSU must be configured with a unique identifier and descriptor that is known by the ERS.

c) It must not be possible to modify the configuration settings of the RSU without an authorized secure logon.

3.3.2 Physical Security

Components of an RSU that may be subject to tampering (i.e. tablet) must utilize a method that will provide evidence of tampering.

3.3.3 Touch Screens

Touch screens shall be accurate once calibrated and shall maintain that accuracy for at least the manufacturer's recommended maintenance period.

3.3.4 Communications

a) An RSU must be designed or programmed such that it may only communicate with authorized ERS components. An RSU will use communication methodologies and technologies as detailed in Chapter 5 – Communications Requirements of this standard:

b) An RSU may use any of the communication technologies noted in Chapter 5 of this standard as a primary means of communication and/or data transfer provided that one or more other technologies are available as a backup in the event of primary communication failure.

c) Communications and/or data transfer must only occur between the RSU and the ERS system via authorized access points.

3.4 Critical Memory Requirements

3.4.1 Critical Memory

Critical memory is used to store all data that is considered vital to the continued operation of the RSU. Critical memory shall be maintained for the purpose of storing and preserving critical data. This includes, but is not limited to:

a) When not communicating with the system, recall of all tickets sold including, at a minimum, draw numbers and validation numbers; and

b) RSU configuration data

Note: *Critical memory may be maintained by any component(s) of the ERS.*

3.4.2 Maintenance of Critical Memory

Critical memory storage shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, time stamps and/or effective use of validity codes.

3.4.3 Comprehensive Checks

It is recommended that critical memory is continuously monitored for corruption, and shall detect failures with an extremely high level of accuracy.

3.4.4 Unrecoverable Critical Memory

An unrecoverable corruption of critical memory shall result in an error. Upon detection, the raffle sales unit shall cease to function.

3.4.5 Backup Requirements

The RSU must have a backup or archive utility, which allows for the recovery of critical data should a failure occur.

3.5 RSU Program Requirements

3.5.1 Identification

All programs shall contain sufficient information to identify the software and revision level of the information stored on the RSU, which may be displayed via a display screen.

Note: *The process used in the identification of the software and revision level will be evaluated on a case-by-case basis.*

3.5.2 Detection of Corruption

RSU programs shall be capable of detecting program corruption and cause the RSU to cease operations until corrected.

Note: *Program verification mechanisms will be evaluated on a case-by-case basis and approved by the ATF laboratory based on industry-standard security policies.*

3.5.3 Verification of Updates

Prior to execution of the updated software, the software must be successfully authenticated on the RSU.

3.6 RSU Management Requirements

3.6.1 RSU Management Functionality

An ERS must have a master list of each authorized RSU in operation, including at a minimum, the following information for each entry:

a) A unique RSU identification number or corresponding hardware identifier (i.e. MAC Address)

b) Operator identification

c) Tickets issued for sale, if applicable

Note: *if these parameters can be retrieved directly from the RSU, sufficient controls must be in place to ensure accuracy of the information.*

3.6.2 RSU Validation

It is recommended that RSUs be validated at pre-defined time intervals with at least one method of authentication. This time interval shall be configurable based on the LGA requirements. The system shall have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

3.7 Independent Control Program Verification

3.7.1 General Statement

The RSU shall have the ability to allow for an independent integrity check of the RSU's software from an outside source and is required for all software that may affect the integrity of the raffle. This must be accomplished by being authenticated by a third-party device, or by allowing for the removal of the media such that it can be verified externally. Other methods shall be evaluated on a case-by-case basis. This integrity check will provide a means of field verification of the software to identify and validate the program. The ATF, prior to device approval, shall evaluate the integrity check method.

Note: *If the authentication program is within the RSU software, the manufacturer of the RSU must receive written approval from the authentication program developer prior to submission and testing by the ATF.*

3.8 RSU Ticket Printer

3.8.1 General Statement

The RSU ticket printer that is used to dispense a paper ticket shall be configured to print the information as detailed in sections 2.2.2.A/B of this standard.

Note: *It may be permissible for some of this information to be contained on the ticket stock itself.*

3.8.2 RSU Printer Configuration

a) The RSU ticket printer must be connected to the RSU sales device using one of communication technologies described in Chapter 5 of this standard as a primary communication method.

b) The RSU must control the transfer of ticket data sent to the RSU printer, and only transfer ticket data to the printer when sufficient space is available in the RSU printer memory to receive the ticket information.

c) If a barcode forms part of the validation number printed on the ticket, the printer must support the barcode format and print with sufficient resolution to permit validation by a barcode reader.

d) The printer must be capable of detecting a low paper/out of paper condition and must cease operation and alert the operator to the need to load new paper.

e) The printer must be capable of detecting a low battery condition and alerting the operator.

f) If the RSU ticket printer is capable of reprinting a ticket, the reprinted ticket shall clearly indicate that it is a reprint of the original ticket.

4 Electronic Raffle System Platform

4.1 Introduction

4.1.1 General Statement

The ERS Platform servers must be located locally, within a single facility. Remote location of the platform server will require the LGA approval.

4.1.2 Asset Management

All assets housing, processing of communication controlled information, including those comprising the operating environment of the Raffle system and/or its components, should be accounted for and have a designated “owner” responsible for ensuring that information and assets are appropriately classified, and defining and periodically reviewing access restrictions and classifications.

4.2 General Operation and Server Security

4.2.1 Physical Security

Servers are to be housed in a secure location (server room) that has physical protection against unauthorized access, for the prevention of alteration or tampering.

4.2.2 Logical Security

a) The ERS must be logically secured by means using generally accepted practices for IT network security which may include but is not limited to one or more of the following technologies:

   i. Passwords,

   ii. PINs

   iii. Authentication credentials (I.e. magnetic swipe, proximity cards, embedded chip cards),

   iv. Biometrics.

b) The ERS must have multiple security access levels to control and restrict different classes of access to the system.

c) The ERS must be configured for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts.

4.2.3 Access Controls

The allocation of access privileges shall be restricted and controlled on business requirements and the principle of least privilege.

a) A formal user registration and de-registration procedure must be in place for granting and revoking access to all information systems and services.

b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

c) The use of generic accounts shall be limited, and where used the reasons for their use shall be formally documented.

d) Password provision must be controlled through a formal management process.

e) Passwords must meet business requirements for length, complexity and lifespan.

f) Access to system applications shall be controlled by a secure log-on procedure.

g) Appropriate authentication methods, in addition to passwords, shall be used to control access by remote users

h) Any physical access to areas housing components used for the sale of raffle ticket(s) through the Internet application and any logical access to these applications must be recorded.

i) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be formally documented and must be included in the regular review of access by Management.

j) Restrictions on connection times shall be used to provide additional security for high-risk applications.

k) The use of utility programs that might be capable of overriding system application controls shall be restricted and tightly controlled.

l) A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

4.2.4 Security from Alteration, Tampers, or Unauthorized Access

The ERS shall provide a logical means of securing the system data against alteration, tampering or unauthorized access. The following rules also apply to the raffle data within the ERS:

a) No equipment shall have a mechanism whereby an error will cause the system data to automatically clear. Data shall be maintained at all times regardless of whether the server is being supplied with power.

b) Data shall be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.

4.2.5 Data Alteration

The ERS shall not permit the alteration of any accounting, reporting or significant event data without supervised access controls. In the event any data is changed, the following information shall be logged, stored and available:

a) Data element altered

b) Data element value prior to alteration

c) Data element value after alteration

d) Time and date of alteration,

e) User that performed the alteration (through login credentials)

4.2.6 Server Programming

The ERS platform must be sufficiently locked down to prevent any user initiated programming capabilities on the server in relation to the ERS application. It is acceptable for a network administrator to perform authorized network infrastructure maintenance or application troubleshooting.

4.2.7 Virus Protection

It is recommended the ERS have adequate and up to date virus protection.

4.2.8 Uninterruptible Power Supply (UPS) Support

a) Where the platform is a stand-alone application, it must have an UPS connected and of sufficient capacity to permit a graceful shut-down and that retains all ERS data during a power loss.

b) It is acceptable that the ERS server may be a component of a network that is supported by a network-wide UPS provided that the ERS server is included as a device protected by the UPS.

4.3 Network Security Management

4.3.1 Network Security

To ensure Purchasers are not exposed to unnecessary security risks by choosing to participate in raffles. Security requirements must apply to the following critical components of the ERS:

a) System components which record, store, process, share, transmit or retrieve sensitive Purchaser information, e.g. credit card/debit card details, authentication information, patron account balances.

b) System components which store results of the current state of a Purchaser's purchase order.

c) Points of entry to and exit from the above systems (other systems which are able to communicate directly with the core critical systems).

d) Communication networks which transmit sensitive patron information.

4.4 System Clock Requirements

4.4.1 System Clock

An ERS must maintain an internal clock that synchronizes with all other system clocks; reflects the current date and time in 24 hour hour format showing hours and minutes; follows changes to daylight saving times; and shall be used to provide the following:

a) Time stamping of significant events

b) Reference clock for reporting

c) Time stamping of all sales and draw events

4.4.2 Synchronization Feature

If multiple clocks are supported, the system shall have a facility to synchronize clocks within all system components.

4.5 Platform (Entry) Printers

4.5.1 General Statement

The configuration of printers used for the printing of entries must have sufficient capacity to print the number of entries based on the expected volume of ticket sales and within the time frame set for the conduct of the event.

4.5.2 Physical (Drum) Printer Configuration

The design of the physical layout of the printers must ensure that all printed entries are available to be drawn using the manual draw process as specified in the Licence rules. With the exception of paper roll changes, the configuration must not rely on any operator intervention to ensure that every printed entry is collected properly in the drum.

4.5.3 Printer Specifications

All printers used in the platform configuration must be capable of printing entries in the format described in sections 2.2.3.A/B of this standard.

4.5.4 Low Paper Condition

a) All printers must have the ability to detect a low paper condition and alert the operator.

b) On detection of a low paper condition,

   i. The printer must have the capacity to complete the current print request.

   ii. The printer must not accept any further print requests and will remain unavailable until the low paper condition has been resolved.

   iii. On resolution, the printer must become available to the system without requiring an operator to reconfigure the printer settings.

b) At no time should a printer be available to the system to print an entry if it is without paper

4.5.5 Printer Disable

At any time during an active draw, the operator must have the ability to manually disable a printer and remove the printer from the configuration without affecting the remaining printers or any outstanding print requests.

4.6 Significant Events

4.6.1 Event Logging

a) Significant events shall be communicated and logged on the ERS server. Significant events include, but are not limited to:

   i. Power reset or failure of any component of the system

   ii. Critical memory corruption of any component of the system

   iii. Entry printer errors, including low paper, out of paper, printer disconnection/failure to print or buffer full.

   iv. Establishment and failure of communication between sensitive ERS components

   v. Significant event buffer full

   vi. Program error or authentication mismatch

   vii. Firewall audit log full, where supported

   viii. Remote access, where supported

   ix. RSU event log

   x. RSU corruption Log

   xi. Any other significant events as specified by the LGA

b) An ERS shall provide an interrogation program that enables on-line comprehensive searching of the significant events log through recorded data. The interrogation program shall have the ability to perform a search using one or more on the following criteria:

   i. Date and time range

   ii. Unique component identification number

   iii. Significant event identifier

4.7 Backups and Recovery

4.7.1 Storage Medium Backup

The ERS shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the raffle can continue. Redundant copies of critical data shall be kept on the ERS with open support for backups and restoration.

a) All storage shall be through an error checking, non-volatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the ERS and the process of auditing those functions can continue with no critical data loss.

b) The database shall be stored on redundant media so that no single failure of any portion of the system would cause the loss or corruption of data.

4.7.2 Recovery Requirements

In the event of a catastrophic failure, when the ERS cannot be restarted in any other way, it shall be possible to reload the ERS from the last viable backup point and fully recover the contents of that backup. The ERS must have the ability to fully reconstruct the event including but not limited to:

a) Sales Data

b) Significant Events

c) Accounting information

d) Reporting information

e) Specific site information such as employee file, raffle set-up, etc

4.8 Data Archiving

4.8.1 General Statement

The ERS must be capable of creating an archival data set for each draw conducted. This data set must contain at a minimum:

a) All of those aspects of standard event reporting as noted in section 2.6.2 of this standard

b) All of those aspects of accounting reporting as noted in section 2.6.3.

4.9 Verification of System Software

4.9.1 General Statement

System software components and modules shall be verifiable by a secure means at the system level denoting Program ID and version. The system shall have the ability to allow for an independent integrity check of the components and modules from an outside source and is required for all software that may affect the integrity of the system. This must be accomplished by being authenticated by a third-party device, or by allowing for the removal of the media such that it can be verified externally. Other methods may be evaluated on a case-by-case basis. This integrity check will provide a means for field verification of the system components and modules to identify and validate the programs or files. The ATF, prior to system approval, shall approve the integrity check method.

***Note**: If the authentication program is contained within the ERS software, the manufacturer of the ERS must receive written approval from the authentication program developer prior to submission.*

4.9.2 Version History Report

The ERS must be capable of generating a report showing the current software revision, date installed, previous (historical) software versions, dates installed and removed. This report should also contain login id and ip/MAC addresses denoting where the commands originated for the actions performed.

5 Communication and Connectivity Requirements

5.1 Introduction

5.1.1 General Statement

An ERS may use one or more of the following methods of communication/connectivity. This is not intended to limit alternate or future technologies:

a) Standard IT network connectivity methods (Ethernet)

b) Cellular

c) Wireless communication protocol commonly known as 802.11(x)

d) Bluetooth

e) Physical connections including proprietary methods (i.e. docking stations)

f) Removable storage media

g) Infrared (IR)

The requirements of this chapter shall also apply if communications are performed across a public or third party network, as approved by the LGA.

5.1.2 Communication Protocol

Each component of an ERS must function as indicated by the communication protocol implemented. Communications shall be demonstrably secure against crypto-analytic attacks. The encryption key(s) used to provide security to the system that provides for the sale of tickets through the Internet must be monitored and maintained. An ERS system must comply with the following:

a) Mutual authentication between any system component and the server where a communication technology is utilized.

b) Protocols that have proper error detection and recovery mechanisms, which are designed to prevent eavesdropping and tampering. Any alternative implementations will be reviewed on a case-by-case basis with LGA approval.

c) Encryption for all communications critical to the raffle:

    i. There must be a documented process for obtaining or generating encryption keys.

    ii. If encryption keys expire there must be a documented process for managing the expiration of the encryption keys.

    iii. There must be a documented process to revoke encryption keys

    iv. There must be a documented process for securely changing the current encryption keyset.

    v. There must be a documented process for the storage of any encryption keys.

    vi. There must be a method to recover data encrypted with a revoked or expired encryption key for a defined period of time after the encryption key becomes invalid.

d) Personally identifiable information, sensitive account data and financial information must be protected over a public network.

e) The failure of any single item should not result in denial of service.

f) An Intrusion Detection System/Intrusion Prevention System must be installed on the network which can:

    i. Listen to both internal and external network activities;

    ii. Detect or prevent Distributed Denial of Services (DDoS) attacks;

    iii. Detect or prevent shellcode from traversing the network;

    iv. Detect or prevent Address Resolution Protocol (ARP) spoofing; and

    v. Detect other Man-in-the-Middle indicators and server communications immediately if detected.

g) Stateless protocols (e.g. UDP) should not be used for sensitive data without stateful transport.

h) All changes to network infrastructure (e.g. network device configuration) must be logged.

i) Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses.

j) Network security should be tested by a qualified and experienced individual on a basis determined by LGA.

k) Testing should include testing of the external (public) interfaces and the internal network.

l) Testing of each security domain on the internal network should be undertaken separately.

Note*: Although HTTP is technically stateless, if it runs on TCP which is stateful, this is allowed.*

5.1.3 Cryptographic Controls

Cryptographic controls must be implemented for the protection of information.

a) Any sensitive or personally identifiable information should be encrypted if it traverses a network with a lower level of trust;

b) Data that is not required to be hidden but must be authenticated must use some form of message authentication technique;

c) Authentication must use a security certificate from an approved organization;

d) The grade of encryption used should be appropriate to the sensitivity of the data;

e) The use of encryption algorithms must be reviewed periodically by qualified Management/Staff to verify that the current encryption algorithms are secure;

f) Changes to encryption algorithms to correct weaknesses must be implemented as soon as practical. If no such changes are available, the algorithm must be replaced; and

g) Encryption keys must not be stored without being encrypted through a different encryption method and/or by using a different encryption key.

5.1.4 Bi-Directional Requirements

Significant emphasis shall be placed on the integrity of the communication system for bi-directional data. With the requirement of “two-way communication” where personal/banking information is transferred bi-directionally through a communication link, the security of the system is paramount. Any system used to sell raffle ticket(s) through the Internet shall ensure that:

a) The physical network is designed to provide exceptional stability and limited communication errors;

b) The system is stable and capable of overcoming and adjusting for communication errors in a thorough, secure and precise manner; and

c) Information is duly protected with the most secure forms of protection via encryption, segregation of information, firewalls, passwords and personal identification numbers.

5.1.5 Connectivity

Only authorized devices shall be permitted to establish communications or connectivity between any system components. The ERS shall provide a method to:

a) Verify that the system component is being operated by an authorized user

b) Enroll and unenroll system components

c) Enable and disable specific system components

d) Ensure that only enrolled and enabled system components participate in the raffle

e) Ensure that the default condition for components shall be unenrolled and disabled

5.1.6 Loss of Communications – RSU

a) It is permitted that RSU's may continue to sell tickets when not in communication with the ERS. Sales transactions taking place on the RSU during a loss of communication with the ERS shall be stored or cached on the RSU. The RSU shall disable sales upon detecting the limit of its buffer overflow or cache limits.

b) Reasonable buffer/cache limits must be established in order that upon re-establishment of communications, the ERS is able to accommodate the load.

c) Upon the re-establishment of communication, the system shall require that the RSU re-authenticates with the ERS and transmits, uploads or otherwise transfers all sales transactions completed during the communication loss.

d) Loss of communications shall not affect the integrity of critical memory.

e) In the event that the primary means of communication is not recoverable within the period of the raffle draw, the RSU must be capable of transmitting, uploading, or otherwise transferring the cached sales data to the ERS using a secondary means of communication.

5.2 System Security

5.2.1 General Statement

Where an ERS is configured for internet connectivity, all communications, including remote access, must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path. Any alternate network path existing for redundancy purposes must also pass through a least one application-level firewall.

5.2.2 Firewalls

a) A firewall should be located at the boundary of any two dissimilar security domains.

b) All connections to hosts used for the sale of raffle tickets through the Internet must be housed in a secure data centre and must pass through at least one application-level firewall. This includes connections to and from any non-related hosts used by the operator.

c) The firewall must be a separate hardware device with the following characteristics:

   i. Only firewall-related applications may reside on the firewall; and

   ii. Only a limited number of accounts may be present on the firewall (e.g. system administrators only).

d) The firewall must reject all connections except those that have been specifically approved.

e) The firewall must reject all connections from destinations which cannot reside on the network from which the message originated (e.g. RFC1918 addresses on the public side of an internet firewall.)

f) The firewall must maintain an audit log of all changes to parameters which control the connections permitted through the firewall.

g) The firewall must maintain an audit log of all successful and unsuccessful connection attempts. Logs should be kept for 90 days and a sample reviewed monthly for unexpected traffic.

h) The firewall must disable all communication if the audit log becomes full.

5.2.3 Firewall Audit Logs

The firewall application must maintain an audit log and must disable all communications and generate a significant event which meets the requirements as specified in section 4.6.1 of this standard, if the audit log becomes full. The audit log shall be capable of being printed on demand and viewable in real time, and must contain:

a) All changes to configuration of the firewall

b) All successful and unsuccessful connection attempts through the firewall

c) The source and destination IP Addresses, port number and MAC addresses

***Note**: A configurable parameter "unsuccessful connection attempts" may be utilized to deny further connection requests should the re-defined threshold be exceeded. The system administrator must also be notified.*

5.3 Remote Access

5.3.1 General Statement

Remote access is defined as any access from outside the system or system network including any access from other networks within the same establishment. Remote access shall only be allowed if authorized by the LGA, otherwise it must be disabled.

5.3.2 Remote Access

a) Where and when permitted, remote access shall accept only the remote connections permissible by the firewall application and ERS settings.

b) The ERS must be configured to deny the following functionality to a remote user:

   i. User administration functionality (adding users, changing permissions, etc.)

   ii. Access to any database other than information retrieval using existing functions,

   iii. Access to the operating system

c) Remote access security and permitted functions during a remote access session will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approved by the LGA.

***Note**: LGA acknowledges that the system manufacturer may, as needed, remotely access the ERS and its associated components for the purpose of product and user support, as permitted.*

5.3.3 Remote Access during a Raffle

Where remote access has been authorized by the LGA, the following conditions apply:

a) The ERS must be capable of disabling remote access during the period of an active raffle game.

b) Remote access during an active raffle event can only be authorized and granted by the local, on-site administrator through the issuance of a temporary password.

5.3.4 Remote Access Auditing

The ERS must maintain an activity log which updates automatically depicting all remote access information, to include:

a) Log on name

b) Time and date the connection was made

c) Duration of the connection

d) Activity while logged in, including the specific areas accessed and any changes that were made

5.3.5 Third Party Hosting

Where one or more components of the ERS are hosted by a third party service provider, the following requirements must be met:

a) The private and financial information of all players must be protected by the third party service provider using industry-standard ISS controls.

b) No third party service may be used which requires software to comply with rules/regulations which are contradictory to any items found within this standard.

5.4 Wide Area Network Communications

5.4.1 General Statement

Wide Area Network (WAN) communications are permitted as approved by LGA and shall meet the following requirements:

a) The communications over the WAN are secured from intrusion, interference and eavesdropping via techniques such as the use of a Virtual Private Network (VPN), encryption, etc.

b) Only functions documented in the communications protocol shall be used over the WAN. The protocol specification shall be provided to the ATF.

5.5 Wireless Network Communications

5.5.1 General Statement

Should a wireless communication solution be utilized, it is recommended to adhere to the applicable portions of the chapter pertaining to wireless networks in the GLI-27 Standard – Network Security Best Practices.

***Note**: Due to continuous changes and improvements in wireless technology, the information in this document is considered current as of the publication date. Therefore, it is imperative for the manufacturer to review and update internal control policies and procedures to ensure the ERS is secure and threats and vulnerabilities are addressed accordingly.*

6 Random Number Generator Requirements

6.1 Introduction

6.1.1 General Statement

The selection process for the winning number shall be random. This may be accomplished through the use of an approved Random Number Generator (RNG). The requirements within this section are only applicable to electronic raffle systems in which a RNG is utilized.

6.2 Random Number Generator (RNG) Requirements

6.2.1 Game Selection Process

An RNG shall reside on a Program Storage Device secured in the logic board of the system. The numbers selected by the RNG for each drawing shall be stored in the system's memory and be capable of being output to produce a winning number.

a) **All Outcomes Shall be Available** - Each valid, sold raffle number shall be available for random selection at the initiation of each drawing.

b) **No Corruption from Associated Equipment** - An electronic raffle system shall use appropriate protocols to protect the random number generator and random selection process from influence by associated equipment, which may be communicating with the electronic raffle system.

c) **RNG Integrity Standard** - The RNG and random selection process shall be impervious to influences from outside the electronic raffle system, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference.

6.3 Electronic Random Number Generator Requirements

6.3.1 General Statement

The use of an RNG results in the selection of raffle outcomes in which the selection shall:

a) Be statistically independent;

b) Conform to the desired random distribution;

c) Pass various recognized statistical tests; and

d) Be unpredictable.

6.3.2 Software

Software pseudo–random number generators must demonstrate the following qualities:

a) the output of the RNG should be unpredictable, for example, for a software RNG it should be computationally infeasible to predict what the next number will be without complete knowledge of the algorithm and seed value;

b) random number generation does not reproduce the same output stream (cycle), and that two instances of a RNG do not produce the same stream as each other (synchronize);

c) any forms of initialization, seeding and re-seeding used do not introduce predictability;

d) cycle (produce output) in the background, unless specifically designed to work "on demand"; and

e) seeding sources should be demonstrably random sources of entropy.

Where a software pseudo-RNG utilizes a mechanical RNG for failover purposes the mechanical RNG must meet the requirements of section 6.4.1

6.3.3 Applied Tests

The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

a) Chi-square test
b) Equi-distribution (frequency) test
c) Gap test
d) Overlaps test
e) Poker test
f) Coupon collector' s test
g) Permutation test
h) Kolmogorov-Smirnov test
i) Adjacency criterion tests
j) Order statistic test
k) Runs tests (patterns of occurrences should not be recurrent)
l) Interplay correlation test
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game)
n) Tests on subsequences
o) Poisson distribution

NOTE: *The independent test lab will choose the appropriate tests on a case by case basis, depending on the RNG under review.*

6.3.4 Period

The period of the RNG, in conjunction with the methods of implementing the RNG outcomes, must be sufficiently large to ensure that all valid, sold numbers are available for random selection.

6.3.5 Range

The range of raw values produced by the RNG must be sufficiently large to provide adequate precision and flexibility when scaling and mapping.

6.3.6 Background RNG Cycling/Activity Requirement

In order to ensure that RNG outcomes cannot be predicted, adequate background cycling / activity must be implemented at a speed that cannot be timed. The rate of background cycling / activity must be sufficiently random in and of itself to prevent prediction.

NOTE: *The test laboratory recognizes that sometime during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this exception shall be kept to a minimum.*

6.3.7 RNG Seeding/Re-Seeding

The methods of seeding or re-seeding implemented in the RNG must ensure that all seed values are determined securely, and that the resultant sequence of outcomes is not predictable.

a) The first seed shall be randomly determined by an uncontrolled event. If a multi-event raffle, after every entry drawn, there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that the selection process will not synchronize.

b) Unless proven to have no adverse effect on the randomness of the RNG outcomes, or actually improve the randomness of the RNG outcomes, seeding and re-seeding must be kept to an absolute minimum. If a multi-event raffle and if for any reason the background cycling / activity of the RNG is interrupted, the next seed value for the RNG must be a function of the value produced by the RNG immediately prior to the interruption.

6.3.8 Winning Number Draw

The winning number selection shall only be produced from sold ticket numbers for the current drawing to be available for selection.

a) For raffles which offer multiple awards or drawings with separate buy-ins for each, the winning number selection shall only be produced from sold ticket numbers corresponding with each applicable award or drawing. As winning numbers are drawn, they shall be immediately used as governed by the rules of the raffle (i.e. the entries are not to be discarded due to adaptive behavior).

6.3.9 Scaling Algorithms

The methods of scaling (i.e. converting raw RNG outcomes of a greater range into scaled RNG outcomes of a lesser range) must be linear, and must not introduce any bias, pattern or predictability. The scaled RNG outcomes must be proven to pass various recognized statistical tests.

a) If a random number with a range shorter than that provided by the RNG is required for some purpose within the raffle system, the method of re-scaling, (i.e., converting the number to the lower range), is to be designed in such a way that all numbers within the lower range are equally probable.

b) If a particular random number selected is outside the range of equal distribution of rescaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

6.4 Mechanical Random Number Generator Requirements

6.4.1 Mechanical Based RNG

If applicable, mechanical based RNGs use the laws of physics to generate the outcome of the game. All mechanical based RNGs must meet the requirements of this document with the exception of the requirements for electronic random number generators. Inherent to their physical nature, the performance of mechanical based RNGs can deteriorate over time. The failure of a mechanical based RNG could have serious consequences for the raffle as raffles may become predictable or exhibit biased distribution. In addition, mechanical based RNG drawings must meet the following rules:

a) The test laboratory will test, via PC communications, multiple iterations to gather enough data to verify the randomness. In addition, the manufacturer may supply live data to assist in this evaluation.

b) The mechanical pieces must be constructed of materials to prevent decomposition of any component over time (e.g., an entry shall not disintegrate).

c) The properties of physical items used to choose the outcome shall not be alterable.

d) No one shall be able to physically interact or come into physical contact or manipulate the device physically housing the mechanical RNG.

e) Some form of dynamic / active, real-time testing of the output is required in the software, such that game play is disabled when an output testing failure is detected.

Where a mechanical RNG utilizes a software pseudo-RNG for failover purposes the pRNG must meet the requirements of sections 6.3.1 and 6.3.2.

NOTE: *Replacement parts may be required after a pre-determined amount of time. In addition, the device(s) may require periodic inspections to ensure the integrity of the device. Each mechanical based RNG game shall be reviewed on a case-by-case basis.*

7 On-line Sales Requirements

7.1 Introduction

7.1.1 General Statement

c) This section is intended to outline those standards that apply to the sale of tickets on-line (through the Internet).

d) An on-line platform used for the sale of ticket(s) through the Internet must provide full audit trail and accounting information needed to determine all sales initiated through the website.

7.1.2 On-line Purchasing

A participant may purchase a ticket from a raffle website by following the instructions appearing on the screen and providing payment for the ticket(s). Each ticket must be sold individually for the price indicated. Multiple discounted prices will only be allowed if a way of ensuring financial accountability is possible by the ERS:

a) A ticket purchase via a credit card transaction or other methods which can produce a sufficient audit trail must not be processed until such time as the funds are received from the issuer or the issuer provides an authorization number indicating that the purchase has been authorized.

b) There must be a clear notification that the purchase has been accepted by the system and the details of the actual purchase accepted must be provided to the patron once the purchase is accepted.

c) Purchase confirmation should include the final amount of the purchase accepted by the ERS on-line platform.

7.1.3 Ticket Issuance

After the payment confirmation, the purchaser shall receive a receipt through the Internet that the purchase of ticket(s) is complete. The purchaser can then receive the ticket(s) bought via e-mail. The receipt acknowledging ticket(s) purchased and the issuance of the tickets, through the Internet, must be processed separately.