

Gaming Policy and Enforcement Branch (GPEB)

TGS6

Technical Gaming Standards for Electronic Raffle Systems

Technical Standards Document (TSD) Version 2.0



Gaming Policy and Enforcement Branch

3rd Floor, 910 Government Street
P.O. Box 9202 Stn. Prov. Govt.
Victoria, British Columbia, Canada
V8W 9J1

© Gaming Policy and Enforcement Branch

All rights reserved. No part of this document may be reprinted, reproduced, stored in a retrieval system or transmitted, in any form or by any means, without prior permission in writing from the Gaming Policy and Enforcement Branch, other than for the internal business use of the British Columbia Lottery Corporation.

Revision Date: January 7, 2016.

Table of Contents

1	Overview of TSD	5
1.1	Introduction.....	5
1.1.1	General Statements I	5
1.1.2	General Statement II.....	5
1.2	Acknowledgment of Other TSDs Reviewed.....	5
1.2.1	General Statement.....	5
1.3	Purpose of TSD.....	5
1.3.1	Purpose.....	5
1.3.2	No Limitation of Technology	6
1.4	Other Documents That May Apply	6
1.4.1	Other TSDs	6
1.4.2	GPEB Standards.....	6
1.4.3	Legislated Acts or Regulations	6
1.4.4	Information Systems Security (ISS) Industry Standards	6
1.5	Definitions.....	7
1.6	Phases of Testing	7
1.6.1	General Statement.....	7
2	Electronic Raffle Systems (ERS) Management	8
2.1	General Operating Procedures	8
2.1.1	General Statement.....	8
2.1.2	Licence Compliance.....	8
2.1.3	Prize Limitations.....	8
2.1.4	Time Limits.....	8
2.1.5	System Configuration Changes	8
2.2	Tickets.....	8
2.2.1	General Statement.....	8
2.2.2	Raffle Tickets – Multiple Event	8
2.2.3	Counterfoil Ticket – Multiple Event Manual Draw	9
2.2.4	Bearer Tickets – Single Event	9
2.2.5	Counterfoil Tickets – Single Event Manual Draw	9
2.2.6	Additional Printed Information.....	10
2.2.7	Validation Numbers.....	10
2.2.8	Voiding a Raffle Ticket.....	10
2.3	Raffle Prize Display	10
2.3.1	Active Jackpot Display	10
2.3.2	Winning Draw Number Display	10
2.4	Closing Sales	11
2.4.1	General Statement.....	11
2.4.2	Time of Closing	11
2.4.3	Closure of RSU's	11
2.4.4	Reconciliation.....	11
2.5	Winner Determination	11
2.5.1	General Statement.....	11
2.5.2	Manually Drawn Counterfoil Validation.....	11
2.5.3	Winner Verification.....	11
2.6	Accounting Reports.....	11
2.6.1	General Statement.....	11
2.6.2	Standard Event Reporting	12
2.6.3	Accounting Reports.....	12
3	Raffle Sales Unit (RSU) Requirements	13
3.1	Introduction.....	13
3.1.1	General Statement.....	13
3.2	RSU Types	13
3.2.1	Attendant-operated RSU	13

3.2.2	Player-Operated RSU:.....	13
3.3	Raffle Sales Unit Operations and Security.....	13
3.3.1	Access Controls.....	13
3.3.2	Physical Security.....	13
3.3.3	Touch Screens.....	13
3.3.4	Communications.....	13
3.4	Critical Memory Requirements.....	14
3.4.1	Critical Memory Defined.....	14
3.4.2	Maintenance of Critical Memory.....	14
3.4.3	Comprehensive Checks.....	14
3.4.4	Unrecoverable Critical Memory.....	14
3.4.5	Backup Requirements.....	14
3.5	RSU Program Requirements.....	14
3.5.1	Identification.....	14
3.5.2	Detection of Corruption.....	14
3.5.3	Verification of Updates.....	15
3.6	RSU Management Requirements.....	15
3.6.1	RSU Management Functionality.....	15
3.6.2	RSU Validation.....	15
3.7	Independent Control Program Verification.....	15
3.7.1	General Statement.....	15
3.8	RSU Raffle Ticket Printer.....	15
3.8.1	General Statement.....	15
3.8.2	RSU Printer Configuration.....	16
4	Electronic Raffle System (ERS) Platform.....	17
4.1	Introduction.....	17
4.1.1	General Statement.....	17
4.2	General Operation and Server Security.....	17
4.2.1	Physical Security.....	17
4.2.2	Logical Security.....	17
4.2.3	Security from Alteration, Tamper, or Unauthorized Access.....	17
4.2.4	Data Alteration.....	17
4.2.5	Server Programming.....	17
4.2.6	Virus Protection.....	18
4.2.7	UPS Support.....	18
4.3	System Clock Requirements.....	18
4.3.1	System Clock.....	18
4.3.2	Synchronization Feature.....	18
4.4	Platform (Counterfoil) Printers.....	18
4.4.1	General Statement.....	18
4.4.2	Physical Printer Configuration.....	18
4.4.3	Printer Specifications.....	18
4.4.4	Low Paper Condition.....	18
4.4.5	Printer Disable.....	19
4.5	Significant Events.....	19
4.5.1	Event Logging.....	19
4.6	Backups, Recovery and Shutdown.....	19
4.6.1	Storage Medium Backup.....	19
4.6.2	Recovery Requirements.....	19
4.6.3	Shutdown Requirements.....	20
4.7	Data Archiving.....	20
4.7.1	General Statement.....	20
4.8	Authentication of System Software.....	20
4.8.1	General Statement.....	20
5	Communication and Connectivity Requirements.....	21
5.1	Introduction.....	21

5.1.1	General Statement.....	21
5.1.2	Communication Protocol.....	21
5.1.3	Connectivity	21
5.1.4	Loss of Communications - RSU.....	21
5.2	System Security	22
5.2.1	General Statement.....	22
5.2.2	Firewall Audit Logs.....	22
5.3	Remote Access	22
5.3.1	General Statement.....	22
5.3.2	Remote Access.....	22
5.3.3	Remote Access During a Raffle.....	22
5.3.4	Remote Access Auditing.....	22
5.4	Wide Area Network Communications	23
5.4.1	General Statement.....	23
5.5	Wireless Network Communications	23
5.5.1	General Statement.....	23
6	Random Number Generator Requirements	24
6.1	Introduction.....	24
6.1.1	General Statement.....	24
6.2	Random Number Generator (RNG) Requirements	24
6.2.1	General Statement.....	24
6.2.2	Applied Tests	24
6.2.3	Period.....	24
6.2.4	Range	25
6.2.5	Background RNG Cycling/Activity Requirement.....	25
6.2.6	RNG Seeding/Re-Seeding.....	25
6.3	Scaling.....	25
6.3.1	Scaling Algorithms	25
6.4	Number Selection Process.....	25
6.4.1	Winning Number Draw.....	25
6.4.2	No Corruption from Associated Equipment	26

1 Overview of TSD

1.1 Introduction

1.1.1 General Statements I

The General Statements are as follows:

- a) Before being permitted to operate in the live environment, all gaming supplies used in the Province of British Columbia must be tested to the applicable requirements set forth in this Technical Standards Document (TSD).
- b) For the purposes of this TSD, Electronic Raffle Systems mean gaming supplies as defined in Section 1 of the Gaming Control Act of British Columbia.
- c) A vendor may select an Accredited Testing Facility (ATF), or other equivalent body, that has been accredited by and registered with the Gaming Policy and Enforcement Branch (GPEB), to perform this testing.
- d) The appointed testing body must provide their final evaluation results, reports, and any additional documentation as may be required directly to GPEB for review, and where required, subsequent discussion.
- e) The vendor may elect to perform internal quality assurance testing on an Electronic Raffle Systems; however, reliance on the test results for the purposes of certification will rest solely with GPEB.
- f) For certainty, any ATF, or other equivalent body, that is employed to perform this testing and is approved by GPEB must essentially treat the vendor as its client, and GPEB 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 British Columbia, the ultimate authority to approve gaming supplies rests solely with GPEB. Only GPEB can issue a Certificate of Technical Integrity under Section 75 of the Gaming Control Act of British Columbia.

1.1.2 General Statement II

It is the policy of GPEB, to update this TSD at minimum once annually, to reflect any changes in technology, testing methods, or known cheating methods.

***Note:** GPEB 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 British Columbia. However, in order to ensure consistency and compliance, GPEB will not modify or selectively apply the requirements set forth in this TSD without first providing reasonable prior written notice to any vendors, on an as-needed and case-by-case basis.*

1.2 Acknowledgment of Other TSDs Reviewed

1.2.1 General Statement

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

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

1.3 Purpose of TSD

1.3.1 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, and
 - 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.

1.3.2 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, GPEB, will review this TSD, make any changes deemed necessary, and incorporate new minimum standards for the new technology.

1.4 Other Documents That May Apply

1.4.1 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 (i.e.: TGS6 – Electronic Raffle Systems),
- b) TGS1 – Technical Gaming Standards for Electronic Gaming Devices (EGDs) in Gaming Venues,
- c) TGS3 – Technical Gaming Standards for On-line Monitoring and Control Systems (MCSs) and Validation Systems in Gaming Venues.

1.4.2 GPEB Standards

This TSD must not contradict any provisions of the following standards:

- a) Advertising and Marketing Standards for the BC Gambling Industry, and
- b) GPEB Responsible Gambling Standards.

1.4.3 Legislated Acts or Regulations

This TSD must not contradict any provisions of the following legislation:

- a) The Criminal Code of Canada,
- b) The Gaming Control Act and Gaming Control Regulation of British Columbia, and
- c) The British Columbia Freedom of Information and Protection of Privacy Act.

1.4.4 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).

1.5 Definitions

- a) ATF (Accredited Testing Facility) - An accredited test facility/laboratory approved by GPEB for the purposes of gaming supply testing.
- b) Bearer Ticket – A specific type of raffle ticket that is used for a single-event raffle and is an electronic record or a paper ticket provided as a transaction receipt that is given to a purchaser and contains one or more draw numbers.
- c) Counterfoil Ticket– means an electronic record or a paper ticket stub, also known as a barrel ticket, which will be manually drawn to determine a winner and contains a single draw number matching the player's bearer ticket, purchased and may, depending on the type of raffle, contain the name, address, or telephone number of the player.
- d) Discounted Tickets – raffle tickets sold in groups containing a specific number of draw numbers at a discounted price (e.g. 3 for \$10, 10 for \$5, etc.)
- e) Draw Number – a uniquely identifiable number that is provided to the purchaser for each chance purchased. Each draw number is printed on a counterfoil and is eligible to be drawn as the winning number for the raffle.
- f) Electronic Raffle System (ERS) means computer software and related equipment used by raffle licensees to sell tickets, account for sales, and facilitates the manual or electronic drawing of tickets to determine the winners.
- g) Multiple Event Raffle – a raffle conducted over the course of more than one day and/or more than one event/location.
- h) Raffle Ticket - means an electronic record or a paper ticket provided as a transaction receipt that is given to a purchaser and contains one or more draw numbers.
- i) RNG – Random Number Generator
- j) RSU – Raffle Sales Unit. 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 raffle tickets.
- k) Single Event Raffle – a raffle conducted on the same day at the same event and location.
- l) 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 may be in the form of a barcode or a human readable form.

1.6 Phases of Testing

1.6.1 General Statement

The approval of an ERS will be certified in two phases.

- a) Initial ATF testing, where the ATF will test the integrity of the system and where necessary the veracity of the RNG (Random Number Generator) in conjunction with supplied Raffle Sales Units, in a laboratory setting with the equipment assembled; and
- b) As required by GPEB, 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 at the venue, and any other tests as mandate by GPEB.

2 Electronic Raffle Systems (ERS) Management

2.1 General Operating Procedures

2.1.1 General Statement

An Electronic Raffle System as defined in Section 1.5(f) will have:

- a) A device or devices that provide for the sale of raffle tickets.
- b) A facility that provides the tools necessary for the collection, tracking, and accounting of all transactions initiated through the raffle system.
- c) The ability to support all Raffle Sales Units (RSU's) whether they are hard-wired or connected wirelessly to ensure that each unit sends or transmits all ticket sales to the system.
- d) A solution that facilitates the printing and collection of counterfoil tickets for use in a manual draw process that ensures that each counterfoil ticket has an equally likely chance to be drawn or
- e) A solution that facilitates the generation of a random winning selection by electronic means from all sold tickets and ensures that each ticket has an equally likely chance to be drawn

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 Limitations

If required by the licence conditions, an ERS must be capable of configuring a limit to the maximum amount that may be won.

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, through a software lock must ensure that once a raffle has commenced, system configuration changes shall not be allowed until the completion of the raffle.

2.2 Tickets

2.2.1 General Statement

An RSU must be capable of generating and printing a raffle ticket with one or more uniquely identifiable draw numbers.

- a) The system must not generate duplicate draw numbers within the same event.
- b) For each draw number generated, there must be one and only one matching counterfoil ticket printed with the same draw number.
- c) The RSU must be capable of providing a transaction receipt in the form of a raffle ticket or bearer ticket to a purchaser.

2.2.2 Raffle Tickets – Multiple Event

After payment of a fee, a purchaser shall receive a printed raffle ticket as a transaction record for one or more chances to win a raffle drawing. A raffle ticket must be printed with the following information at a minimum:

- a) Name and address of the licensee and year-round contact phone number;
- b) Gaming event licence number, to be shown as "BC Gaming Event Licence # _____";
- c) Location, date and time of all draws, including early bird draws'
- d) One or more unique draw numbers generated by the ERS and printed by the RSU for each purchased ticket;
- e) Purchase date and time (in twenty-four (24) format showing hours and minutes)
- f) Number of tickets printed in each price category, if applicable;
- g) Price of the ticket;
- h) RSU identifier from which the ticket was generated;
- i) Statement of required presence at the draw as a condition of winning, if applicable;
- j) The words "Winners consent to the release of their names by the licensee."
- k) (Licence Classes A and C): the statement, "Ticket purchasers must be 19 years of age or older. If a winning ticket bears a minor's name, the prize will be lawfully delivered on behalf of the minor to the minor's parent, legal guardian or trustee."

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)*

2.2.3 Counterfoil Ticket – Multiple Event Manual Draw

All counterfoil tickets used in a Multi-event raffle manual drawing must be printed and stored electronically for each purchased draw number. The printed counterfoil tickets must be the same size, shape, and weight. The system must generate a unique counterfoil ticket for each draw number generated by an RSU for a sold raffle ticket. A counterfoil ticket must be printed with the following information, at a minimum;

- a) The name, address and telephone number of the ticket purchaser;
- b) One draw number which exactly matches a single draw numbers from the raffle ticket issued to the purchaser;
- c) Gaming event licence number, to be shown as "BC Gaming Event Licence # _____";
- d) Purchase date and time (in twenty-four (24) format showing hours and minutes)
- e) If required, a unique validation number or barcode.

2.2.4 Bearer Tickets – Single Event

Single event raffle tickets, commonly used for meat draws and 50/50 draws can utilize a special type of raffle ticket known as a bearer ticket. After payment of a fee, a purchaser shall receive a printed bearer ticket as a transaction record for one or more chances to win the raffle draw. (See Section 1.5 (C) – Discounted tickets). A bearer ticket must be printed with the following information at a minimum:

- a) Name of the licensee;
- b) Event Identifier or Location;
- c) Gaming event licence number, to be shown as "BC Gaming Event Licence # _____";
- d) One or more unique draw numbers generated by the ERS and printed by the RSU for each purchased ticket;
- e) Purchase date and time (in twenty-four (24) format showing hours and minutes);
- f) RSU identifier from which the ticket was generated;
- g) Price of the Ticket;
- h) Unique Validation number or barcode.

Note: *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)*

2.2.5 Counterfoil Tickets – Single Event Manual Draw

All counterfoil tickets used in a single event raffle manual drawing must be printed and stored

electronically for each purchased draw number. The printed counterfoil tickets must be the same size, shape, and weight. The system must generate a unique counterfoil ticket for each draw number generated by an RSU for a sold raffle ticket. A counterfoil ticket must be printed with the following information at a minimum:

- a) Event Identifier or Location;
- b) One draw number which exactly matches a single draw number from the raffle ticket (bearer ticket) issued to the purchaser;
- c) Purchase date and time (in twenty-four (24) format showing hours and minutes);
- d) Unique Validation number or barcode.

2.2.6 Additional Printed Information

It is permissible that a raffle ticket (or bearer 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 and 2.2.4 of this standard. It is not recommended that counterfoil tickets have any additional printed information.

2.2.7 Validation Numbers

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

2.2.8 Voiding a Raffle Ticket

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

- a) Raffle tickets must be voided within the ERS platform application by the system administrator or authorized personnel. It must not be possible to void a ticket from an RSU.
- b) If a raffle 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.
- c) Voided draw numbers shall not be available for resale or re-issue.
- d) The ERS must flag or otherwise identify in the system, a voided raffle ticket and its corresponding draw number(s) in support of the winning number validation process.
- e) The ERS must require an acknowledgement by the system administrator or authorized personnel that voided tickets have been reconciled before permitting a winning number to be entered into the system.

2.3 Raffle Prize Display

2.3.1 Active Jackpot Display

For ERS's that support a display of the current jackpot that is intended to be viewed by purchasers of the raffle in the location of the raffle, that display shall indicate the raffle prize in Canadian Dollars using a calculation deemed acceptable to GPEB and that represents the current progression of the prize.

***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 conduct of the draw*

2.3.2 Winning Draw Number Display

For ERS's that support a display of the winning draw number that is intended to be viewed by participants of the raffle in the location of the raffle, that display shall indicate the winning draw number in the same format as the printed counterfoil draw number 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 be capable of closing off the sale of raffle tickets at a time to be determined by the licensee. No ticket sales may occur after the raffle purchase period has been closed.

2.4.2 Time of Closing

The time of the sales closing may be:

- a) Configurable within the ERS
- b) Manually enabled by the Licensee.

2.4.3 Closure of RSU's

The ERS must be capable of displaying to the licensee by way of the RSU device display that all sales within a particular RSU have been uploaded, transferred or otherwise communicated to the ERS.

- a) On verification of the sales data transfer, the RSU device must be capable of being reset or closed
- b) The RSU must not be enabled for any further sales for the current raffle.

2.4.4 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 manual or electronic draw which ensures a randomly selected draw number is chosen from all tickets sold during the period of the raffle and complies with all rules and standard procedures as stipulated in their license.

2.5.2 Manually Drawn Counterfoil Validation

On completion of a manual draw, the ERS must have the facility to verify the status of the drawn counterfoil 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 for winning number within the system database.

2.6 Accounting Reports

2.6.1 General Statement

The ERS must be capable of producing exportable general accounting reports 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, etc.)
- d) Prize distribution
 - i. Prize award to winning participant
 - ii. Revenue retained by Licensee
- e) Refund totals by event
- f) Draw numbers-in-play count
- g) Winning number. .

2.6.3 Accounting Reports

- a) The ERS must, at a minimum be capable of producing the following general accounting reports in an exportable format: Error/Exception Report –Exception information including, but not limited to, changes to the raffle configuration, corrections, overrides, and voids.
- b) Raffle Ticket Report – A report which includes a list of all raffle ticket sold including all associated draw numbers, selling price and RSU identifier.
- c) Sales by RSU – A report which includes a breakdown of each RSU's total sales, including draw numbers generated and any voided or misprinted tickets or reprint requests.
- d) Voided Draw Number Report – A report which includes a list of all draw numbers that have been voided including corresponding validation numbers.

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 generate and print raffles tickets as described in Section 2.2.2 and Section 2.2.4 of this standard.
- b) Raffle Tickets may be purchased either from an attendant-operated RSU or a player-operated RSU. Any other methods will be reviewed and approved by GPEB on a case-by-case basis.

3.2 RSU Types

3.2.1 Attendant-operated RSU

- a) Raffle tickets may sold by an attendant. Upon receiving payment for the ticket, the attendant will cause the RSU to generate and print a raffle ticket (or bearer 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) Raffle tickets are sold by 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 and dispense or cause to be delivered a raffle ticket (or bearer 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. The software must have the ability to automatically lock up or logoff after a system -configurable amount of inactivity.
- b) An RSU must be configured with a unique identifier 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 Defined

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 GPEB 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 must receive written approval from the authentication program vendor prior to submission and testing by the ATF.

3.8 RSU Raffle Ticket Printer

3.8.1 General Statement

The RSU ticket printer that is used to generate a paper raffle (or bearer) ticket shall be configured to print the information as detailed in Section 2.2.2 and 2.2.4 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 raffle ticket and/or bearer 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 (ERS) 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 GPEB approval.

4.2 General Operation and Server Security

4.2.1 Physical Security

The servers shall be housed in a secure location that has sufficient physical protection against alteration, tampering or unauthorized access.

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 Security from Alteration, Tamperers, 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.

4.2.4 Data Alteration

The ERS must not permit the alteration of any accounting, reporting or significant event data. In the event any data is changed, the following information shall be documented or logged:

- 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)

4.2.5 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.

4.2.6 Virus Protection

It is recommended all servers and RSU's have adequate and up to date virus protection.

4.2.7 UPS Support

- a) Where the platform is a stand-alone application, it must have an Uninterruptible Power Supply (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 System Clock Requirements

4.3.1 System Clock

An ERS must maintain an internal clock that reflects the current date and time (in twenty-four (24) hour format showing hours and minutes) that 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

4.3.2 Synchronization Feature

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

4.4 Platform (Counterfoil) Printers

4.4.1 General Statement

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

4.4.2 Physical Printer Configuration

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

4.4.3 Printer Specifications

- d) All printers used in the platform configuration must be capable of printing counterfoil tickets in the format described in Section 2.2.5 of this standard.

4.4.4 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.
- c) At no time should a printer be available to the system to print a counterfoil ticket without

paper.

4.4.5 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.

4.5 Significant Events

4.5.1 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 an RSU or any component of the system
 - ii. Critical memory corruption of any component of the system
 - iii. Counterfoil printer errors, including low paper, out of paper, printer disconnection/failure or print buffer overflow
 - 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 GPEB
- 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

4.6 Backups, Recovery and Shutdown

4.6.1 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.

4.6.2 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

4.6.3 Shutdown Requirements

The ERS must have the following shutdown and recovery capabilities:

- a) The ERS must be able to perform a graceful shutdown with no loss of data and only allowing automatic restart after the following minimum requirements have been met on power up:
 - i. Program resumption routine(s) including self-tests that complete successfully
 - ii. All critical control program components of the ERS have been authenticated and
 - iii. Communication with all ERS components have been established and authenticated
- b) The ERS must be able to identify and handle the situation where master resets have occurred on system components.
- c) The ERS must have the ability to recover all critical information from the last backup and
- d) If a system failure should occur, all critical information from the time of the last backup to the point in time that the system failure occurred should be recoverable.

4.7 Data Archiving

4.7.1 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.

4.8 Authentication of System Software

4.8.1 General Statement

System software components and modules shall be authenticated 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 authenticated externally. Other methods may be evaluated on a case-by-case basis. This integrity check will provide a means for field authentication 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 must receive written approval from the authentication program vendor prior to submission.*

5 Communication and Connectivity Requirements

5.1 Introduction

5.1.1 General Statement

An ERS may use one or more the following methods of communication/connectivity. This is a representative sample and 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 GPEB.

5.1.2 Communication Protocol

Each component of an ERS must function as indicated by the communication protocol implemented. An ERS system must provide for 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 GPEB approval.
- c) Encryption for all communications critical to the raffle. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

5.1.3 Connectivity

Only authorised 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 un-enroll 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 un-enrolled and disabled

5.1.4 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 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 4.5 - (Significant Events) of this standard if the audit log becomes full. The audit log shall 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 GPEB, 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 GPEB.

Note: GPEB 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

- 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 game 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

5.4 Wide Area Network Communications

5.4.1 General Statement

Wide Area Network (WAN) communications are permitted as approved by GPEB 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. The regulations within this section are only applicable to electronic raffle systems in which a Random Number Generator is utilized.

6.2 Random Number Generator (RNG) Requirements

6.2.1 General Statement

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

6.2.2 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; and
- 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.*

6.2.3 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.

6.2.4 Range

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

6.2.5 Background RNG Cycling/Activity Requirement

In order to ensure that RNG outcomes cannot be predicted, adequate background cycling/activity must be implemented between each drawing 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 some times during the raffle, the RNG may not be cycled when interrupts may be suspended. This is permitted although this exception shall be kept to a minimum.*

6.2.6 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. After every bearer ticket draw, 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 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 Scaling

6.3.1 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 re-scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

6.4 Number Selection Process

6.4.1 Winning Number Draw

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

- a) Each valid, sold raffle number shall be available for random selection at the initiation of each drawing;
- b) For raffles which offer multiple awards or drawings with separate buy-ins for each, the winning number selection shall only be produced from sold bearer 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 bearer tickets are not to be discarded due to adaptive behavior).

6.4.2 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.