CHAPTER 2

2.0 RAFFLE MANAGEMENT REQUIREMENTS

2.1 Introduction

2.1.1 General Statement. Each electronic raffle system shall have a device or facility that provides for the sale of bearer tickets and the collection and accounting tools needed to track all sales initiated through the raffle system. The system must have the ability to support all Raffle Sales Units (RSUs) whether they are hard-wired or connected wirelessly to ensure that each unit sends or transmits all ticket sales to the system. The system must have the ability to facilitate winner selection by either manual or electronic means.

2.2 Raffle Configuration

2.2.1 Prize Limitations. The electronic raffle system software must be capable of being configured with a limit or cap on the prize of a raffle drawing which may apply to the maximum amount that may be won.

2.2.2 Time Limits. The electronic raffle system software must be capable of setting time limits for when tickets may be purchased for a raffle drawing.

2.2.3 ***Configuration Changes.*** After the commencement of a raffle, the electronic raffle system software shall not allow changes to parameters which may affect the integrity of the raffle.

2.3 Bearer Ticket Issuance

2.3.1 Bearer Tickets. After the payment of a fee, participants shall receive a bearer ticket for one or more chances to win a raffle drawing. The bearer ticket must be printed with the following information (at minimum):

a) Name of organization conducting the raffle
b) Event Identifier or Location;
c) One or more unique draw number(s) purchased for the raffle.
d) Issued date and time (in twenty-four (24) hour format showing hours and minutes);
e) RSU identifier from which the ticket was generated;
f) Value or cost of the bearer ticket;
g) Unique validation number or barcode; and
h) License number, if applicable;

NOTE: *It may be permissible for some or all of this information to be contained on the ticket stock itself. Where a series of raffles is conducted by a single operator, tickets for each raffle must be differentiated from the other tickets used in the series.*

2.3.2 Validation Numbers. The algorithm or method used by the electronic raffle system to generate the bearer ticket validation number must be unpredictable and ensure against duplicate validation numbers for the raffle currently in progress.

2.3.3 Voiding a Ticket. The electronic raffle system must flag or otherwise identify a voided bearer ticket and its corresponding draw number(s). The system shall record at a minimum the draw numbers and the validation number from the voided bearer ticket. Voided draw numbers shall not be able to be resold or reissued for that raffle.

2.3.4 Additional Printed Information. It is permissible that a 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 2.3.1 of this standard.

2.4 Counterfoil Requirements

2.4.1 Counterfoils. Where a manual draw is used to determine a winner, all counterfoils used in a raffle drawing must be the same size, shape, and weight. A counterfoil shall be printed or stored electronically for each purchased draw number. If an electronic random number generator is used to determine the winner of the raffle drawing, a printed counterfoil is not required. A counterfoil must only contain one draw number and shall contain the following information, which matches the bearer ticket issued to the player:

a) Event Identifier or Location**;**
b) The draw number
c) Issued date and time (in twenty-four (24) hour format showing hours and minutes);
d) Value or cost of the bearer ticket; and
e) Unique validation number or barcode;

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

2.4.2 Reprinting of Counterfoils. Where the system supports the reprinting of counterfoil tickets, this facility shall require additional supervised access controls (e.g. password) and the draw numbers for all reprinted counterfoils shall be flagged in the system as reprints.

2.5 Raffle Prize Display Requirements

2.5.1 Raffle Prize Displays. For systems that support a raffle prize display that is intended to be viewed by participants of the raffle, that display shall indicate the raffle prize in local monetary value using a calculation deemed acceptable by the regulatory body, and represent the current progression of the prize.

NOTE: *It is accepted that, depending on the medium, communication delays are variable and beyond the knowledge or control of the operator, and the displayed prize amount may be different from the amount recognized in the system.*

2.5.2 Alternating Displays. If applicable, it is sufficient to have multiple raffle awards displayed in an alternating fashion.

2.6 Raffle Drawing Requirements

2.6.1 General Statement. A raffle drawing shall be held at a date, time, place, and in a manner determined by the operator and/or regulatory agency. A raffle drawing shall only be conducted after:

a) The close of the raffle; and
b) All sales and voided sales for the particular raffle purchase period have been reconciled.

2.6.2 Closing the Raffle Purchase Period. The system must be capable of closing off the sale of bearer tickets at a time determined by the operator. No sales of tickets may occur after the raffle purchase period has been closed. The system must be capable of displaying to the operator by way of the RSU device display that all sales from a particular device have been uploaded, transferred or otherwise communicated to the electronic raffle system.

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.

2.6.3 Voided Tickets. Voided tickets shall not be qualified toward any prize. The system must be capable of reconciling voided sales for the raffle purchase to identify all voided tickets which may be committed to the draw. The system must record an acknowledgement from the event manager that voided tickets have been reconciled before permitting a winning number to be entered into the system for validation.

2.6.4 Winner Determination. The operator shall conduct a manual, electronic, or other approved draw procedure which ensures a randomly selected draw number as a winner from all tickets sold. Each drawn counterfoil shall be verified as a sold and valid ticket. This process shall be repeated for each advertised prize.

2.6.5 Official Drawing Results. Results of the drawing become official and final after the drawn number is verified as a winning bearer ticket for the respective drawing, and is presented to the participants of the raffle. The system shall display the winning draw on all capable display devices that are intended to be viewed by participants.

2.7 Winning Ticket Redemption

2.7.1 Winner Verification. Winning tickets shall be verified prior to payout. Participants must present the bearer ticket to an authorized agent for validation with the system. The system must be capable of verifying the winning draw numbers and shall allow for the validation of draw numbers either manually or through the use of a bar code scanner or equivalent.

NOTE: *Amounts won that exceed any jurisdictional specified limit shall require the appropriate documentation to be completed before the winning participant is paid.*

2.8 Electronic Accounting and Reporting

2.8.1 System Reporting Requirements. The system or other equipment shall be capable of producing general accounting reports to include the following information for each draw conducted:

a) Raffle Drawing Report. A report which includes the following for each raffle drawing:
   i. Date and time of event.
   ii. Organization running the event.
   iii. Sales information (sales totals, refunds, etc).
   iv. Prize value awarded to participant
   v. Prize distribution (total raffle sales vs. prize value awarded to participant)
   vi. Refund totals by event.
   vii. Draw numbers-in-play count.
   viii. Winning number(s) drawn (including draw order, call time, and claim status).

b) Exception Report. A report which includes system exception information, including, but not limited to, changes to system parameters, corrections, overrides, and voids.

c) Bearer Tickets Report. A report which includes a list of all bearer tickets sold including all associated draw numbers, selling price, and RSU identifier.

d) Sales by RSU. A report which includes a breakdown of each RSU's total sales (including draw numbers sold) and any voided and misprinted tickets.

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

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

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

CHAPTER 3

3.0 RAFFLE SALES UNIT (RSU) REQUIREMENTS

3.1 Introduction

3.1.1 General Statement. After the payment of a fee, participants shall receive a chance to win a raffle drawing. A chance to win a raffle drawing may be purchased either from an attendant-operated Raffle Sales Unit (RSU) or, as allowed by the regulatory body, a player-operated RSU. Any other methods will be reviewed on a case-by-case basis, as allowed by the regulatory body.

a) Attendant-Operated Raffle Sales Unit: A participant may purchase a bearer ticket from an attendant-operated RSU by providing payment for the ticket(s) to the attendant. Upon receiving payment, the attendant will provide the participant the bearer ticket(s) purchased by the participant.

b) Player-Operated Raffle Sales Unit: A participant may purchase a bearer ticket from a player-operated RSU by following the instructions appearing on the screen of the RSU and providing payment for the ticket(s). Upon payment for the ticket(s), the RSU will issue the corresponding bearer ticket(s) purchased by the participant.

3.2 Raffle Sales Unit Operations and Security

3.2.1 General Statement. An RSU must be capable of generating and printing a bearer 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 corresponding counterfoil with the same draw number.

c) The RSU must be capable of providing a transaction receipt in the form of a bearer ticket to a purchaser.

3.2.2 Access Controls. Access to raffle sales software shall be controlled by a secure logon procedure. It must not be possible to modify the configuration settings of the RSU without an authorized secure logon.

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

3.2.4 RSU Interface. The functions of all buttons, touch or click points represented on the RSU interface shall be clearly indicated within the area of the button, or touch/click point and/or within the help menu. There shall be no functionality available through any buttons or touch/click points on the RSU that are undocumented.

3.2.5 Communications. A Raffle Sales Unit must be designed or programmed such that it may only communicate with authorized Electronic Raffle Systems components. The electronic raffle system must have the capability to uniquely identify and authorize each RSU used to sell tickets for a raffle.

3.2.6 Wireless Raffle Sales Units. Communication must only occur between the RSU and the Electronic Raffle System via authorized access points.

3.3 Bearer Ticket Printers

3.3.1 Printing Bearer Tickets. If the RSU connects to a printer that is used to produce bearer tickets, the bearer ticket shall include information as indicated in section 2.3.1. It may be permissible for some of this information to be contained on the ticket stock itself.

a) The RSU must control the transfer of ticket data sent to the printer, and only transfer

ticket data to the printer when sufficient space is available in the printer memory to receive the ticket information.

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

3.3.2 Printer Error Conditions. The bearer ticket printer shall be able to detect and indicate to the operator the following error conditions:

a) Low battery;
b) Out of paper/paper low;
c) Printer disconnected - It is permissible for the system to detect this error condition when it tries to print.
d) If the unit is capable of reprinting a ticket, the reprinted ticket shall clearly indicate that it is a reprint of the original ticket.

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 minimum, draw numbers and validation numbers; and
b) RSU configuration data.

NOTE: *Critical memory may be maintained by any component(s) of the Electronic Raffle System.*

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. Comprehensive checks of critical memory shall be made on startup 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 capability, which allows 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 independent test laboratory based on industry-standard security practices.*

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

3.6 Independent Control Program Verification

3.6.1 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 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 for field verification of the software to identify and validate the program. The test laboratory, 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 regulatory body prior to submission and testing by the test laboratory.*

CHAPTER 4

4.0 RANDOM NUMBER GENERATOR REQUIREMENTS

4.1 Introduction

4.1.1 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.

4.2 Random Number Generator (RNG) Requirements

4.2.1 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.

4.2.2 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.*

4.2.3 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.

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

4.2.5 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.*

4.2.6 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.

4.3 Scaling

4.3.1 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.

4.4 Number Selection Process

4.4.1 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).

4.4.2 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.

CHAPTER 5

5.0 ELECTRONIC RAFFLE SYSTEM SERVERS

5.1 Introduction

5.1.1 General Statement. The Electronic Raffle System Server(s) may be located locally, within a single facility or may be remotely located outside of the facility through a Wide Area Network (WAN) as allowed by the regulatory body.

5.2 General Operation & Server Security

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

5.2.2 Logical Access Control. The electronic raffle system shall be logically secured through the use of passwords, biometrics, or other means as agreed upon between the regulatory body and the operator. The storage of passwords, PINs, biometrics, and other authentication credentials (e.g. magnetic swipe, proximity cards, embedded chip cards) shall be secure. The system must have multiple security access levels to control and restrict different classes of access to the electronic raffle system.

5.2.3 Security from Alteration, Tampering, or Unauthorized Access. The electronic raffle system shall provide a logical means for securing the raffle data against alteration, tampering, or unauthorized access. The following rules also apply to the raffle data within the Electronic Raffle System:

a) No equipment shall have a mechanism whereby an error will cause the raffle 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.

5.2.4 Data Alteration. The Electronic Raffle System 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 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; and
e) Personnel that performed alteration (user login).

5.2.5 Server Programming. There shall be no means available for an operator to conduct programming on the server in any configuration (e.g. the operator should not be able to perform SQL statements to modify the database). However, it is acceptable for Network Administrators to perform authorized network infrastructure maintenance with sufficient access rights, which would include the use of SQL statements that were already resident on the system.

5.2.6 Copy Protection. Copy protection to prevent unauthorized duplication or modification of software, for servers or RSUs, may be implemented provided that:

a) The method of copy protection is fully documented and provided to the Test Laboratory, who will verify that the protection works as described; or
b) The program or component involved in enforcing the copy protection can be individually verified by the methodology described in section 5.7.1.

5.2.7 ***UPS Support***. Where the server 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 electronic raffle system data during a power loss. It is acceptable that the electronic raffle system server may be a component of a network that is supported by a network-wide UPS provided that the server is included as a device protected by the UPS.

5.3 System Clock Requirements

5.3.1 ***System Clock*****.** An Electronic Raffle System 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 for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of all sales and draw events.

5.3.2 ***Synchronization Feature*****.** If multiple clocks are supported the system shall have a facility to synchronize clocks within all system components.

5.4 RSU Management Requirements

5.4.1 ***RSU Management Functionality*****.** An Electronic Raffle System must have a master list of each authorized RSU in operation, including at minimum the following information for each entry:

a) A unique RSU identification number or corresponding hardware identifier (i.e. MAC);
b) Operator identification; and
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.*

5.4.2 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 jurisdictional requirements. The system shall have the ability to remotely disable the RSU after the threshold of unsuccessful validation attempts has been reached.

5.5 Counterfoil Printers

5.5.1 Counterfoil Printers. Where printed counterfoils are in use, the printer mechanism shall be able to detect and indicate the following error conditions:

a) Out of paper - It is permissible for the system to detect this error condition when it tries to print.
b) Paper low - It is permissible for the system to not lock up for these conditions; however, there should be a means for the attendant to be alerted;
c) Memory Error;
d) Printer failure; and
e) Printer disconnected - It is permissible for the system to detect this error condition when it tries to print.

5.5.2 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.

5.6 Significant Events

5.6.1 Event Logging. Significant events shall be communicated and logged on the electronic raffle system, which may include:

a) Connection/Disconnection of an RSU or any component of the system;
b) Critical memory corruption of any component of the system.
c) Counterfoil Printer errors:
    i. Out of paper/paper low;
    ii. Printer disconnect/failure; and
    iii. Printer memory error.
f) Establishment and failure of communications between sensitive Electronic Raffle System components.
g) Significant event buffer full;
h) Program error or authentication mismatch;
i) Firewall audit log full, where supported.
j) Remote access, where supported; and
k) Any other significant events as specified by the regulatory agency.

5.6.2 Surveillance/Security Functionality. Each significant event conveyed to the electronic raffle system must be stored. An Electronic Raffle System shall provide an interrogation program that enables on-line comprehensive searching of the significant events through recorded data. The interrogation program shall have the ability to perform a search based at least on the following:

a) Date and time range;
b) Unique component identification number; and
c) Significant event identifier.

5.7 Backups and Recovery

5.7.1 Storage Medium Backup. The electronic raffle system 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 electronic raffle system with open support for backups and restoration.

a) All storage shall be through an error checking, nonvolatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the electronic raffle system 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.

5.7.2 Recovery Requirements. In the event of a catastrophic failure when the electronic raffle system cannot be restarted in any other way, it shall be possible to reload the electronic raffle system from the last viable backup point and fully recover the contents of that backup, including, but not limited to:

a) Significant Events;
b) Accounting information;
c) Reporting information; and
d) Specific site information such as employee file, raffle set-up, etc.

5.8 Verification of System Software

5.8.1 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 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 test laboratory, prior to system approval, shall approve the integrity check method.

NOTE: *If the authentication program is contained within the Electronic Raffle System software, the manufacturer must receive written approval from the test laboratory prior to submission.*

CHAPTER 6
6.0 COMMUNICATION REQUIREMENTS

6.1 Introduction

6.1.1 General Statement. This chapter will discuss the various communication methods including, but not limited to wireless communications protocol commonly known as 802.11(x) and will extend these methodologies to other wireless interfaces such as Bluetooth, infrared (IR), and cellular (i.e. HSPA+, LTE, etc). The requirements of this chapter shall also apply if communications are performed across a public or third party network, as allowed by the regulatory agency.

6.1.2 Communication Protocol. Each component of an electronic raffle system must function as indicated by the communication protocol implemented. An electronic raffle system must provide for the following:

a) Communication between all system components must provide mutual authentication between the component and the server.
b) All protocols must use communication techniques 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 regulatory approval; and
c) All data communications critical to the raffle shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication.

6.1.3 Connectivity. Only authorized devices shall be permitted to establish communications between any system components. Electronic raffle systems 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; and
e) Ensure that the default condition for components shall be un-enrolled and disabled.

6.1.4 Loss of Communications. Raffle sales units (RSUs) may continue to sell tickets when not in communication with the system, as allowed by the regulatory body. Sales taking place on the RSU during a loss of communication with the system shall be logged on the device. The RSU shall deactivate upon detecting the limit of its buffer overflow. Upon the re-establishment of communication, the system shall require the RSU to re-authenticate with the server(s). All tickets sold during communication loss shall be transmitted to the system. Loss of communications shall not affect the integrity of critical memory.

6.2 System Security

6.2.1 General Statement. 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 at least one application-level firewall.

6.2.2 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 5.5, 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; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

NOTE: *A configurable parameter 'unsuccessful connection attempts' may be utilized to deny further connection requests should the predefined threshold be exceeded. The system administrator must also be notified.*

6.3 Remote Access

6.3.1 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 regulatory body and shall have the option to be disabled. Where allowed, remote access shall accept only the remote connections permissible by the firewall application and electronic raffle system settings. Remote access security will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the local regulatory agency. In addition, there shall be:

a) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
b) No unauthorized access to any database other than information retrieval using existing functions; and
c) No unauthorized access to the operating system.
d) For systems using an electronic RNG, the electronic raffle system must immediately detect remote access.

NOTE: *GLI acknowledges that the system manufacturer may, as needed, remotely access the Electronic Raffle System and its associated components for the purpose of product and user support, as permitted.*

6.3.2 Remote Access Auditing. The electronic raffle system 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 connection; and
d) Activity while logged in, including the specific areas accessed and changes that were made.

6.4 Wide Area Network Communications

6.4.1 General Statement. Wide Area Network (WAN) communications are permitted as allowed by the regulatory body and shall meet the following requirements:

a) The communications over the WAN are secured from intrusion, interference and eavesdropping via techniques such as use of a Virtual Private Network (VPN), encryption, etc; and
b) Only functions documented in the communications protocol shall be used over the WAN. The protocol specification shall be provided to the Testing Laboratory.

6.5 Wireless Network Communications

6.5.1 General Statement. Should a wireless communication solution be utilized, it is recommended to adhere to the following requirements

a) Segregation of Networks. Networks used by the electronic raffle systems should be separate and not include other devices that are not part of the electronic raffle system.
b) Service Set Identifier (SSID). The wireless network name (SSID) used to identify the wireless network should be hidden and not broadcast.
c) Media Access Control (MAC) Address Filtering. The wireless network should use MAC address filtering as means to validate whether or not a device may connect to the wireless network.

d) Device Registration. The electronic raffle system should use a device registration method as means to validate whether or not a device is an authorized device on the electronic raffle system.

NOTE: *Due to continuous changes and improvement in wireless technology the information in this document is considered current as of the publication date. Therefore, it is imperative for organizations to review and update internal control policies and procedures to ensure the electronic raffle system is secure and threats and vulnerabilities are addressed accordingly. GLI recommends the use of a private independent IT security company to plan, inspect and verify the integrity of the wireless network.*