STANDARD SERIES

GLI-13:

On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos

Version: 2.0

Release Date: April 20, 2007

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, Inc.** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, Inc. will provide a certificate evidencing the certification to this Standard.

On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos

GLI-13 Revision 2.0

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, Inc. will provide a certificate evidencing the certification to this Standard.

Date Released: April 20, 2007 Rev 2.0 *Final*
Date Released: June 30, 2006 Rev 1.2 *Released for comment*
Date Created: February 20, 2001 Rev 1.1

REVISION HISTORY

Rev 2.0

Rev 1.2 *Final* was renamed to **Rev2.0** *Final* for document control purpose.

Rev 1.2

General – all references to "EGD" has been changed to refer to "Gaming Device", also, added reference to the Wireless Security Standards outlined within the new Chapter 7, throughout the document. References to "Bill Acceptors" were changed to "Bill Validators" throughout the document. References to "Tickets" were changed to "Ticket/Vouchers" throughout the document to remain consistent with GLI-11 referencing.

1.4. Added clarification to include gaming devices that use player account cards (cashless) to be evaluated against this standard where applicable.

1.5.1(c) removed the reference to "Cashless Systems Standards for Advanced Communication Protocols in Casinos (GLI-14) currently not released" and replaced with Cashless Systems in Casinos GLI-16

1.5.1(d) inserted GLI-17.

1.5.1(e) inserted GLI-18, pushing Internal Controls down to (f) of this section.

1.5.1(g) added a reference to GLI-20 Redemption Terminals for systems that have redemption terminals (kiosks) integrated for ticket/voucher validation.

2.6.2 clarified 'where applicable' since some of the programs may reside in a file where it is not possible to label it.

2.6.2(e) referenced 'or other system device' to clarify the location of installation information needed for system firmware submission requirements to not limit to the interface element.

3.1.2 Modified the Metering Requirements to accommodate multiple rollovers that may occur at the same time.

3.2.1 was changed to require critical information be contained if the FEP maintains buffered/logging information.

3.3.3 clarified that the MCS clocks shall be synchronized, where conflicting information could occur.

3.4.2 was changed to better clarify since the hand pay message is 'confirmed' instead of 'authorized' as previously indicated. In addition, the rule now also refers to the 10425 in addition to the W2G.

3.4.3(a) changed the reference for Alphanumeric Slip Identifier toType of Slip. The Slip Identifier information requirement is now referenced within (b
3.4.3(b) added the requirement for a Numeric Slip identifier (which increments per event).

3.4.3(i) added the reference to Additional Pays, if applicable, to be included on the JP/Fill slip generated by the system.

3.4.4(c) modified the wording pertaining to significant event number to also allow a significant even identifier since previously, the rule would only allow for 'numbers.'

3.4.5(a) changed the rule to refer to the unique interface element'/location' identification number, instead of the previous language which referred to the 'EGD' identification number where the rule topic is based on the device file.

3.4.6 modified the rule to allow for other means to allow controlled access to all accounting information where the previous version specified 'an application.' Also, changed the reference to require all Internal Control required reports to clarify, if these reports are specified.

4.1.1 changed the rule to require the system to function as indicated by the communication protocol to ensure that all ranges of communications permitted by the protocol are supported by the system.

4.1.1 (c) Added a disclaimer to the Communication Protocol section that requires the device to accurately function as indicated by the communication protocol that is implemented.

4.2.1 (a) (b) Clarified (a) and (b) and (c) OR (d) are required.

4.2.1(c) changed the requirement for a unique 'code' to also allow for a unique 'number' to define the event. Also, changed 'and' to 'or' and the end of this rule to give the option of using the unique number/code to define the even or use brief text to describe the event. The previous wording would require both methods.

4.2.2(c) clarified that the system is to receive messages from the Gaming Device for storage for any external door that provides access to a critical area. Previously, the wording would require all accesses be reported and stored however there are areas on the device that do not contain any critical data or elements that would affect the integrity of the Gaming Device.

4.2.2(i) clarified the Printer Errors as meaning Printer Empty/Paper Low; and Printer Disconnect/Failure.

4.2.3 (c) clarified that the memory corruption of the interface element only needs to be reported as a priority event if the element contains critical information. Also added statement regarding the ability to generate a general tilt.

4.3.1 Added meters shall be labeled in accordance to their function

4.3.2 Restructured this section and changed various metering requirements

4.4.2 Changed the statement where the types of reports that are typically run to remove the reference to Weekly reports and added reference to 'Life to Date' reports.

4.4.2(a) changed the reference to Net Win Reports to also refer to 'Revenue' reports since this terminology is used in some areas.

4.4.2(b) removed the requirement for Monthly EGD Revenue Report since the schedule of reports are to be determined by the Gaming Commission. The items within this bulleted list pertain to the information that is to be listed within the reports.

4.4.2(c) was changed to clarify the information needed for the Drop Comparison Reports to include the dollar and percent variances for each medium and aggregate for each type.

4.4.2(d) added clarification for this report to include the dollar and percent variances for each and aggregate

4.4.2(g) changed requirement for Taxation Reports to "other reports" that may be required for the jurisdiction since some do not require Taxation Reports.

4.4.2 NOTE was included to clarify that it is acceptable to combine reporting data where appropriate (e.g., revenue, theoretical/actual comparison).

4.6.3 NOTE was modified to clarify that the rule is referring to the system executable code only.

4.6.4 NOTE was modified to require Remote Access to be optional to accommodate those jurisdictions that do not permit remote access.

4.6.5 Added section on Verification of System Software and clarified that system modules/components must be verified by a third-party device

4.7.2(d) was changed to include the 'employee file' as specific site information that is to be backed up.

5.2 Removed section pertaining to Ticket Information, which are the EGD requirements and made this section on Ticket/Voucher Issuance, which pertains to the validation system**.**

5.2.2 (a)&(b) were added to clarify that the algorithm used must be robust enough to ensure minimal repetition of validation numbers.

5.2.4 was changed to allow for the Gaming Device to allow a max of two off-line ticket/vouchers or handpay receipt since some use the preferable method of forcing handpays in the event there is a loss of communication. Also noted that this section will be re-evaluated and revised once the G2S protocol has been adopted and becomes utilized by the gaming device suppliers

5.3.1 was previously Ticket Issuance, which was removed since, deemed EGD requirements. This section now reflects Online Ticket/Voucher Redemption

5.3.2 is now RESERVED. This section was previously regarding Online Ticket Redemption, which is now covered under 5.3.1

5.3.3(a), (b) & (c) clarified that the cashier may scan the barcode or manually input the validation number and print a validation receipt, if applicable. Previously the bulleted items (a)-(c) required all three actions, incorrectly instead of treating them as two different methods. Also, clarified the printing of a validation receipt is optional.

5.3.4(e) included the reference to a Change Booth identifier if Validation Receipts are supported, in addition to the previously referred to Cashier identifier.

5.3.5(a) changed the reference to invalid Serial Number to invalid Ticket/Voucher, to remain consistent with regard to the terminology used throughout the document.

5.3.7 Added a subsection that refers to GLI-20 Redemption Terminals for systems that integrate this type of device.

5.4.1 noted that this section will be re-evaluated and revised once the G2S protocol has been adopted and becomes utilized by the gaming device suppliers

5.4.1(d) changed the name of the Ticket Drop Report to Ticket/Voucher Drop Variance Report.

5.4.1(e) removed the requirement for Jackpot Ticket Report.

5.4.1(g) clarified that the Cashier Report is to detail individual ticket/vouchers and the sum of the ticket/vouchers paid. Also clarified that this report would pertain to the Cashier and Change Booth and Validation Terminals.

5.4.1 NOTE has been modified to refer to bulleted item number (b) with regard to the bulleted items that are to be waived for two part ticket/vouchers.

6.3.1 (c) and (d) removed the requirement for Radio Frequency Interference and Magnetic Interference testing to be conducted by GLI since it is disclosed that it is the sole responsibility of the manufacturer to comply with any regulations related to the aforementioned. GLI claims no liability and makes no representation with respect to such non-gaming testing.

Table of Contents

CHAPTER 1

1.0 OVERVIEW - STANDARDS FOR MONITORING AND CONTROL SYSTEMS (MCS)

1.1 Introduction

1.1.1 ***On-line Monitoring and Controls System Defined***. An On-line Monitoring and Control System (MCS) is a game management system that continuously monitors each Electronic Gaming Device via a defined communication protocol by either a dedicated line, dial-up system, or other secure transmission method. An MCS is primarily tasked to provide logging, searching, and reporting of gaming Significant Events, collection of individual device financial and meter data, reconciliation of meter data against hard and soft counts, and System Security outlined in section 4.0 of this document.

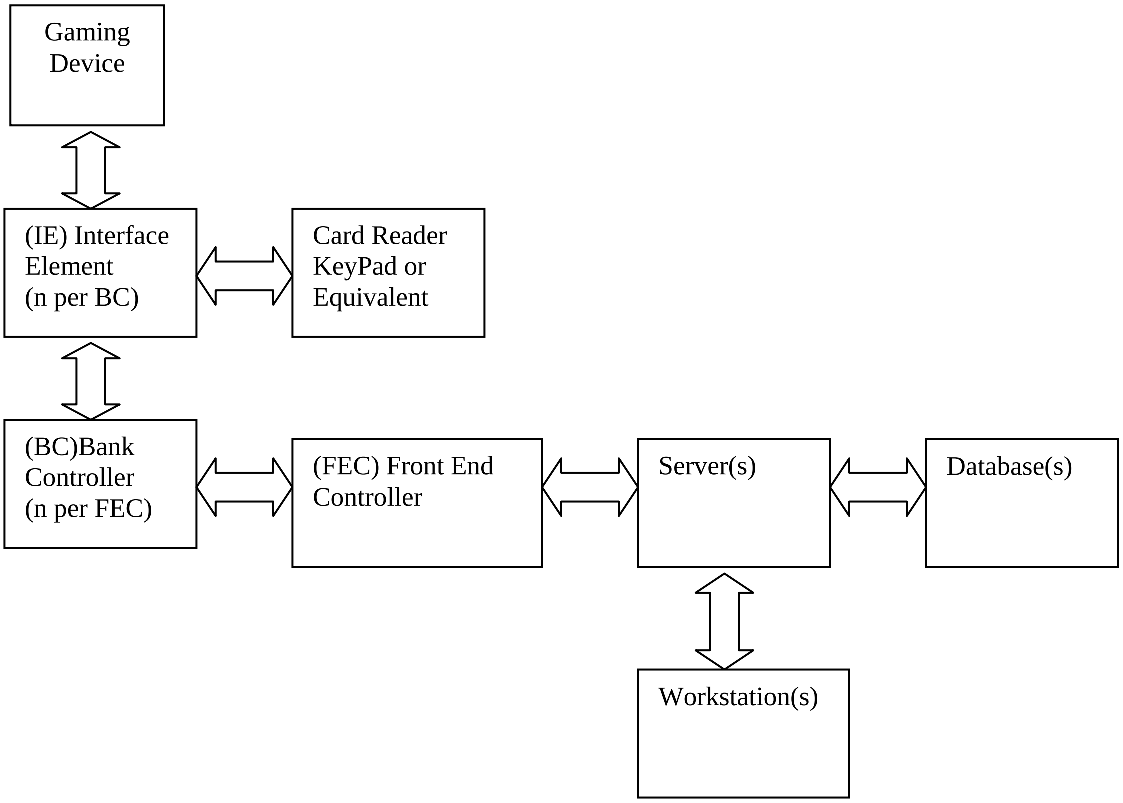
1.1.2 ***Phases of Certification***. The approval of an On-line Monitoring and Control System shall be certified in two phases:

a) Initial laboratory testing, where the laboratory will test the integrity of the system in conjunction with Gaming devices, in the laboratory setting with the equipment assembled; and

b) On-site certification where the communications and set up are tested on the casino floor prior to implementation.

1.2 Graphical Overview

1.2.1 ***General Statement***. The purpose of this section is to lend a visual depiction of a generic On-line Monitoring and controls computer system and is not intended to mandate any particular component or system topology providing functionality is maintained. The terms used throughout this document will be represented in a block diagram format to clarify individual components.


Gaming Device
(IE) Interface Element (n per BC)
Card Reader KeyPad or Equivalent
(BC)Bank Controller (n per FEC)
(FEC) Front End Controller
Server(s)
Database(s)
Workstation(s)

In the illustration above, this standard applies to all components referenced other than the Gaming Device. The requirements for the Gaming Device are defined in GLI-11. This document will only concern communications from the Gaming Device to the MCS, and not in the reverse order, with the exception of the Ticket/Voucher Validation System Requirements that are incorporated within Chapter 5.

1.3 Acknowledgment of Other Standards Reviewed

1.3.1 ***General Statement***. These Standards have been developed by reviewing and using portions of the documents from the organizations listed below. We acknowledge the regulators who have assembled these documents and thank them:

a) The ACT Office of Financial Management;
b) The New South Wales Department of Gaming and Racing;
c) The New Zealand Casino Control Authority;
d) The New Zealand Department of Internal Affairs, Gaming Racing & Censorship Division;
e) The Northern Territory Racing and Gaming Authority;
f) The Queensland Office of Gaming Regulation;
g) The South Australian Office of the Liquor and Gaming Commissioner;
h) The Tasmanian Department of Treasury and Finance, Revenue and Gaming Division;
i) The Victorian Casino and Gaming Authority;
j) The Western Australian Office of Racing Gaming and Liquor;
k) The SABS 1718 part 3;
l) US Tribal Compacts from Tribal Governments and State Governments included:
   i. Arizona
   ii. Connecticut
   iii. Iowa Indian
   iv. Kansas
   v. Louisiana
   vi. Michigan
   vii. Minnesota
   viii. Mississippi
   ix. North Carolina
   x. North Dakota
   xi. Oregon

xii. Wisconsin

m) Colorado Division on Gaming – Limited Gaming Regulations;

n) Illinois Gaming Board – Adopted Rules;

o) Indiana Gaming Commission;

p) Iowa Racing and Gaming Commission;

q) Louisiana State Police – Riverboat Gaming Division – Gaming Device;

r) Missouri Gaming Commission – Department of Public Safety;

s) Nevada Gaming Commission and State Gaming Control Board;

t) New Jersey – Regulations on Accounting and Internal Controls; and

u) South Dakota Commission on Gaming – Rules and Regulations for Limited Gaming.

1.4 Purpose of Standard

1.4.1 ***General Statement***. The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying gaming Monitoring and Control System operation.

b) To only test those criteria which impact the credibility and integrity of gaming from both the Revenue Collection and game play point of view.

c) To create a standard that will insure that On-Line Monitoring and Control Systems (MCS) And Validation Systems in Casinos are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set their public policy with respect to gaming.

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

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

g) To construct a standard that does not specify any particular technology, method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

1.4.2 ***<u>No Limitation of Technology</u>***. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

1.4.3 ***<u>Scope of Standard</u>***. This standard will only govern On-Line Monitoring and Control Systems (MCS) and Validation System requirements necessary to achieve certification when interfaced to Gaming Devices, for the purpose of communicating mandatory security events and electronic meters. This infers that all relevant monetary transactions at the Gaming Device level are handled through:

a) <u>Credit Issuance:</u>
   i. Coins or tokens accepted via approved coin acceptors;
   ii. Currency notes (Bills) accepted via approved bill validators; and
   iii. Approved Ticket/Voucher (Items) accepted via approved bill/ Ticket/Voucher validators or
   iv. Player Account Cards (cashless)

b) <u>Credit Redemption:</u>
   i. Coins or tokens paid by approved hoppers;
   ii. Handpays; and
   iii. Ticket/Voucher (Items) paid by approved ticket/voucher printers or
   iv. Player Account Cards (cashless)

1.4.4 ***<u>Exceptions to Standard</u>***. This standard does not govern MCS requirements for any other form of monetary transaction. This standard also does not govern advanced bi-directional communication protocols (i.e. EFT, Bonusing, Promotional, System Based Progressives, features that utilize an RNG, etc.) that support credit transfer between Gaming Device and MCS. This standard only supports one-way communication of events originated at the Gaming Device level to the MCS with the exception of the Ticket/Voucher Validation System Requirements that are incorporated within Chapter 5. This standard does not exclude Gaming Devices that operate with Player Account Cashless transactions for the purpose of communicating mandatory security events and electronic meters. This infers that all relevant monetary transactions at the EGD level are handled through electronic transfer through a secure communication protocol. These device types shall meet the applicable requirements set forth herein, specifically governing metering information and significant events in addition to other GLI standards that may apply.

1.5 Other Documents That May Apply

1.5.1 ***<u>General Statement</u>***. This standard covers the minimal requirements of an MCS and all associated components. Please refer to the GLI website at www.gaminglabs.com for other GLI Standards. Below are a few that may apply:

a) Gaming devices in Casinos (GLI-11);
b) Progressive Gaming devices in Casinos (GLI-12);
c) Cashless Systems in Casinos (GLI-16);
d) Bonusing Systems in Casinos (GLI-17);
e) Promotional Systems in Casinos (GLI-18);
f) Individual Gaming Commission Minimum Internal Control Procedures; and
g) Redemption Terminals (GLI-20)

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 Introduction

2.1.1 ***General Statement***. This chapter shall govern the types of information that are, or may be required to be submitted by the submitting party in order to have equipment tested to this Standard. Where the information has not been submitted or is not otherwise in the possession of the test laboratory, the submitting party shall be asked to supply additional information. Failure to supply the information can result in denial in whole or in part of the submission and/or lead to testing delays.

2.1.2 ***Previous Submission***. Where the testing laboratory has been previously supplied with the information on a previous submission, duplicate documentation is not required, provided that the previous information is referred to by the submitting party, and those documents are easily located at the testing laboratory. Every effort shall be made to reduce the redundancy of submission information.

2.2 Prototype (Full Submission) Submissions

2.2.1 ***General Statement***. A Prototype (full submission) submission is a first time submission of a particular piece of hardware or software that has not previously been reviewed by the test laboratory. For Modifications of previous submissions, including required changes to previously submitted Prototype (full submission) certification, whether certified or pending certification, see 'Submissions of Modifications (partial submissions) to a Previously Certified Item,' Section 2.7.

NOTE: Due to abnormal component complexity and/or excessive cost it is sometimes necessary for on-site testing of a system at the manufacturer's facility. Regular upgrades *normally preclude testing at the manufacturers' facility except in the case of prototype submissions.*

2.2.2 <u>Submission Letter Requirements</u>. Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by the test laboratory. The letter should include the following:

a) The jurisdiction(s) for which you are requesting certification;
b) The items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of proprietary hardware, the submitting party shall indicate the manufacturer, model, and part and revision numbers of the associated components of hardware; and
c) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

2.3 System Hardware Submission Requirements – Prototype (Full Submission) Certification

2.3.1 <u>Presentation of Equipment to The Test Laboratory; Identical Equipment</u>. Each item of gaming equipment supplied by a manufacturer to the field shall be functionally identical to the specimen tested and certified. For example, an interface element supplied as a certified device shall not have different internal wiring, components, firmware, circuit boards, circuit board track cuts or circuit board patch wires from the certified specimen, unless that change is also certified, see also '<u>Submissions of Modifications (partial submissions) to a Previously Certified Item</u>,' Section 2.7.'

2.3.2 <u>Inventory of Equipment to The Test Laboratory</u>. Each submission of hardware shall contain the following:

a) Server, Database, Front End Controller, Data Collector and Ancillary Stations to include but not limited to: Jackpot/Fill functionality; Surveillance/Security monitor functionality; Gaming Device Management functionality; and Accounting/Reporting Functionality;

b) Monitors, keyboards, mouse, printers, etc., to support the items listed above;

c) Minimum of seven interface element devices with corresponding power connectors (if separate from harness), keypads, and displays;

d) Minimum of one wiring harness for each Gaming Device type desired for operational approval with system where specific harnessing is required;

e) Minimum of two of each type magnetic cards (or equivalent if an alternative media is used) used in the system, if applicable;

f) Network cabling, hubs, switches and any wireless components that may be installed at a casino property; and

g) Un-interruptible Power Supply (UPS) for critical components.

NOTE: In an effort to reduce system submission size, monitor and data switches may be used. Additionally, separate software may be housed in the same unit, as long as the functionality is not impaired and the software is identical to the field version.

2.3.3 Accompanying Documentation. All accompanying technical documents, manuals, and schematics shall be submitted. In addition, the following items shall be provided:

a) If applicable, all UL, CSA, EC, AS3100, etc. or equivalent certification, see also 'Hardware and Player Safety,' Section 6.2. This certification information may be supplied at a later date;

b) Any other proprietary equipment that may be used in the field in conjunction with the Submission, if necessary to test the requirements set forth;

c) Accompanying software, see also 'System Software Submission Requirements – Prototype (Full Submission) Certification,' Section 2.4; and

d) If the submitting party has specialized equipment and/or software which is needed by the test laboratory to test submitted system, such as load/game simulators or test data files, then the specialized equipment and/or software and all appropriate operation and user manuals for the equipment and/or software shall be included with the submission.

NOTE: Commercially available products are not required for submission unless omission will impact testing and proper operation of the system.

2.4 System Software Submission Requirements – Prototype (Full Submission) Certification

2.4.1 ***<u>General Statement</u>***. Each submission of software shall contain the following:

a) Two sets of all EPROMs, CD-ROMs, or other storage media which contain identical contents. This includes all program executables, system component firmware, bin files, etc. Where the test laboratory already has tested a software component, resubmission may not be necessary;

b) Source Code, a Link Map and Symbol Table for all primary software executables. In addition, if requested, explanation of all non-volatile RAM on any system device with the non-volatile RAM locations described;

c) All user manuals in both hard and soft copy format to include a general overview of the system from a component level, software and hardware setup and integration, and system block diagrams and flow charts for the communication program, if required;

d) If not included in the user manuals, a connectivity manual for all unique electronic Gaming Devices capable of being interfaced with system to include device model numbers and compatibility list, if applicable; wiring diagrams depicting connection points to devices, power, etc.; and identification by part number or some other scheme, any unique wiring harnesses, ancillary boards required for communication of a particular device;

e) If not included in the user manuals, provide example reports for each standard report capable of being generated on the system with a formula summary detailing all reporting calculations including data types involved, mathematical operations performed, and field limit;

f) If not included in the user manuals, a list of all supported communication protocols specifying version, if applicable;

g) If utilizing a software verification algorithm provide a description of the algorithm, theoretical basis of the algorithm, results of any analyses or tests to demonstrate that the algorithm is suitable or the intended application, rules for selection of algorithm coefficients or "seeds", and means of setting the algorithm coefficients or "seeds;" and

h) If completed by the manufacturer provide a system test plan and results to detail electronic Gaming devices and software versions tested with.

2.5 Software Programming Requirements and Compilation

2.5.1 ***General Statement***. The following items shall be contained within all submitted source code or related modules:

a) Module Name;

b) Brief description of module function; and

c) Edit History, including who modified it, when and why.

2.5.2 ***Source Code Commented***. All source code submitted shall be commented in an informative and useful manner.

2.5.3 ***Source Code Completeness***. All source code submitted shall be correct, complete and able to be compiled.

2.6 Program Identification

2.6.1 <u>Software Requirements</u>. On the primary system software components submitted and subsequently placed in the field, each program shall be uniquely identified and either display version information at all times or utilizing a user accessible function.

2.6.2 <u>Firmware Requirements</u>. On the system firmware submitted and subsequently placed in the field, each program, where applicable, shall be uniquely identified, displaying:

a) Program ID ;
b) Manufacturer;
c) Version number;
d) Type and size of medium (requirement can be met by manufacturer stamp) ; and
e) Location of installation in interface element or other system device, if potentially confusing.

NOTE: For EPROM based firmware, the identification label shall be placed over the UV window to avoid erasing or alteration of the program.

2.7 Submissions of Modifications (Partial Submissions) to a Previously Certified Item

2.7.1 <u>General Statement</u>. For any update submission (e.g., a revision to an existing hardware or software that is currently under review, certified or has been reviewed and not certified), the following information shall be required to process the submission in addition to the requirements set forth in 'Submission Letter Requirements,' Section 2.2.2. All modifications require re-testing, examination, and re-certification by the test laboratory.

2.7.2 ***Modification of Hardware***. Each hardware submission shall:

a) Identify the individual items being submitted (including part number);
b) Supply a complete set of schematics, diagrams, data sheets, etc. describing the modification along with the reason for the change(s); and
c) Provide the updated or new hardware, a description and the method of connection to the original system or hardware components.

2.7.3 ***Modification of System Software Functions or to Correct Software Error***. The submitter should use the same requirements as in the 'Software Submission Requirements – Prototype (Full Submission) Certification' Section listed above, except where the documentation has not changed. In this case, a resubmission of identical documents is not required. However, the submission must include a description of the software change(s) and modules affected, and new source code for the entire program, if applicable

2.7.4 ***Software Submission - Modification to Existing or Create New System Functionality***. For a system specific submission (e.g., new workstation software), the following information may be required to process the submission:

a) If new, a complete description of the function, including amendment manual and user documents, and new source code if applicable; and
b) If modifying, the submission must include a description of the software change(s), modules affected and new source code, if applicable.

2.8 System Security Submission Requirements

2.8.1 ***General Statement***. Where a system requires the use of defined user roles with associated passwords or pin numbers, a default list of all users and passwords or pin numbers must be submitted including a method to access the database.

2.9 Joint Venture Submissions

2.9.1 ***General Statement***. A system is considered a joint venture when two or more companies are involved in the manufacturing of one system. Due to the increasing amount of joint venture submissions (more than one supplier involved in a product submission) and to alleviate any confusion to the suppliers, our regulator clients and our firm, GLI has set forth the following procedures for such submissions.

a) One company will prepare and submit the entire submission, even if they are using parts from other suppliers, and must identify all part numbers of all components. This will be the primary contact for the submission.

b) The company submitting an approval request should do so on their letterhead. GLI will delegate an internal file number in this company's name and will bill this company for all costs incurred throughout the approval process.

c) The primary contact will be called when questions arise. However, GLI engineers will work with all parties involved, completing the review.

d) All suppliers who are part of the submission "group" may need to be licensed in the jurisdiction(s) where the submission is being approved. As a courtesy to the supplier, GLI may inquire as to whom does not need to be licensed from the regulator client. It should be noted that licensing questions should be handled directly with the jurisdiction.

e) Upon completion, it is the primary contact company that will receive the approval letter, provided the submission meets the jurisdictional requirements. The primary contact company may then release copies of the approval letter to the associated manufacturer(s).

CHAPTER 3

3.0 SYSTEM COMPONENT REQUIREMENTS

3.1 Interface Element Requirements

3.1.1 ***General Statement***. Each Gaming Device installed in the casino must have a device or facility (interface element) installed inside a secure area of the Gaming Device, that provides for communication between the Gaming Device and an external Data Collector.

3.1.2 ***Metering Requirements***. If not directly communicating Gaming Device meters, the interface element must maintain separate electronic meters, of sufficient length, to preclude the loss of information from meter rollovers, or a means to identify multiple rollovers, as provided for in the connected Gaming Device. These electronic meters should be capable of being reviewed on demand, at the interface element level via an authorized access method, see also Section 4.3 'Meters.'

3.1.3 ***Battery Backup Requirements***. The interface element must retain the required information after a power loss for a period determined by the regulatory agency. If this data is stored in volatile RAM, a battery backup must be installed within the interface element, see also Section 4.3 'Meters.'

3.1.4 ***Information Buffering and Integrity Checking***. If unable to communicate the required information to the MCS, the interface element must provide a means to preserve all mandatory meter and significant event information in until at such time as it can be communicated to the MCS, see also Section 4.2, 'Significant Events' and Section 4.3 'Meters.' Gaming Device operation may continue until critical data will be overwritten and lost. There must be a method to check for corruption of the above data storage locations.

3.1.5 Address Requirements. The interface element must allow for the association of a unique identification number to be used in conjunction with a Gaming Device file on the MCS. This identification number will be used by the MCS to track all mandatory information of the associated Gaming Device. Additionally, the MCS should not allow for duplicate Gaming Device file entry of this identification number.

3.1.6 Configuration Access Requirements. The interface element setup/configuration menu(s) must be not be available unless using an authorized access method.

3.2 Front End Controller and Data Collector Requirements

3.2.1 General Statement. A MCS may possess a Front End Processor (FEP) that gathers and relays all data from the connected Data Collectors to the associated database(s). The Data Collectors, in turn, collect all data from, connected Gaming Devices. Communication between components must be via an approved method and at minimum conform to the Communication Protocol requirements stated in Section 4.1 of this document. If the FEP maintains buffered/logging information, then a means shall exist which prevents the loss of critical information contained herein.

3.3 Server and Database Requirements

3.3.1 General Statement. A MCS will possess a Server(s), networked system or distributed systems that direct overall operation and an associated database(s) that stores all entered and collected system information.

3.3.2 System Clock. A MCS must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date 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 configuration changes.

3.3.3 ***Synchronization Feature***. If multiple clocks are supported the MCS shall have a facility whereby it is able to update those clocks in MCS components, whereby conflicting information could occur.

3.3.4 ***Database Access***. The MCS shall have no built-in facility whereby a casino user/operator can bypass system auditing to modify the database directly. Casino Operators will maintain secure access control.

3.4 Workstation Requirements

3.4.1 ***Jackpot/Fill Functionality***. A MCS System must have an application or facility that captures and processes every hand pay message from each Gaming Device. Hand pay messages must be created for single wins (jackpots), progressive jackpots and accumulated credit cash outs (canceled credits), which result in hand pays. A Fill (deposit of a predetermined, or otherwise properly authorized, token amount in a Gaming Device's hopper) is normally initiated from a hopper empty message while a Credit (removal of excess tokens from a Gaming Device) is normally user initiated. An allowable exception to fill initiation would be where the system provides preventative or maintenance fill functionality, in which the transaction may be initiated by the system or an authorized user. Once captured, there must be adequate access controls to allow for authorization, alteration, or deletion of any of the values prior to payment or execution.

3.4.2 ***Tax Reporting Threshold***. Every single win event hand pay message confirmed at this application by personnel of proper authorization, equal to or greater than the tax reporting threshold (established by the US Internal Revenue Service, currently $1,200), must advise the user of the need for a W2G (domestic players) or 10425 (foreign players) (required by the US Internal Revenue Service only) to be processed, either via the MCS or manually. This option must not be capable of being overridden. The keyed reset ability to return winnings from a taxable event to a Gaming Device should require user intervention to void the original jackpot slip that is generated.

NOTE: This is only applicable for U.S. jurisdictions that must comply with taxation requirements.

3.4.3 Jackpot/Fill Slip Information. The following information is required for all slips generated with **some/all** fields to be completed by the MCS:

a) Type of slip;
b) Numeric Slip identifier (which increments per event);
c) Date and Time (Shift if required) ;
d) Gaming Device number;
e) Denomination;
f) Amount of Fill;
g) Amounts of Jackpot, Accumulated Credit, and Additional Pay;
h) W2G indication, if applicable;
i) Additional Payout, if applicable;
j) Total before taxes and taxes withheld, if applicable;
k) Amount to Patron;
l) Total coins played and game outcome of award;
m) Soft meter readings; and
n) Relevant signatures as required by Gaming Board.

NOTE: Items 'b' through 'f,' 'm,' and 'n' apply to fill slips and items 'b' through 'e' and 'g' through 'n' apply to jackpot slips. The above information may vary dependent upon the jurisdictional Internal Controls and may or may not be required.

3.4.4 ***Surveillance/Security Functionality***. A MCS shall provide an interrogation program that enables on-line comprehensive searching of the significant event log for the present and for the previous 14 days through archived data or restoration from backup where maintaining such data on a live database is deemed inappropriate. The interrogation program shall have the ability to perform a search based at least on the following:

a) Date and Time range;
b) Unique interface element/Gaming Device identification number; and
c) Significant event number/identifier.

3.4.5 ***Gaming Device Management Functionality***. A MCS must have a master "Slot file" which is a database of every Gaming Device in operation, including at minimum the following information for each entry. If the MCS retrieves any of these parameters directly from the Gaming Device, sufficient controls must be in place to ensure accuracy of the information.

a) Unique interface element/location identification number;
b) Gaming Device identification number as assigned by the casino;
c) Denomination of the Gaming Device (please note that the denomination may reflect an alternative value, in the case of a multi-denomination game);
d) Theoretical hold of the Gaming Device; and
e) Control program(s) within Gaming Device.

3.4.6 ***Accounting Functionality***. A MCS must have an application or facility that allows controlled access to all accounting (financial) information and shall be able to create all mandatory reports in the 'Reporting Requirements,' Section 4.4, as well as all Internal Control required reports, if specified.

3.4.7 ***<u>Exclusions</u>***. Generally, any system (component) not specified in this document that impacts revenue reporting must be submitted to the laboratory for test. For example, Standalone Player Tracking Systems are not required for submission unless their function includes embedded feature(s) that affect revenue. However, they may be tested for operation and version control if an integrated feature of a MCS submission.

CHAPTER 4

4.0 SYSTEM REQUIREMENTS

4.1 Communication Protocol

4.1.1 ***General Statement***. The system must support a defined communication protocol(s) and function as indicated by the communication protocol(s). A MCS must provide for the following:

a) All critical data communication shall be protocol based and/or incorporate an error detection and correction scheme to ensure an accuracy of ninety-nine percent (99%) or better of messages received;
b) All critical data communication that may affect revenue and is unsecured either in transmission or implementation shall employ encryption. The encryption algorithm shall employ variable keys, or similar methodology to preserve secure communication; and
c) All communication performed within the system, in it's entirety, must accurately function as indicated by the communication protocol that is implemented.

4.2 Significant Events

4.2.1 ***General Statement***. Significant events are generated by a Gaming Device and sent via the interface element to the MCS utilizing an approved communication protocol. Each event must be stored in a database(s), which includes the following:

a) Date and time which the event occurred; and
b) Identity of the Gaming Device that generated the event; and
c) A unique number/code that defines the event; or
d) A brief text that describes the event in the local language.

4.2.2 Significant Events. The following significant events must be collected from the Gaming Device and transmitted to the system for storage:

a) Power Resets or power failure;

b) Hand pay Conditions (amount needs to be sent to the system):
   i. Gaming Device Jackpot (An award in excess of the single win limit of the Gaming Device);
   ii. Cancelled Credit Hand pay; and
   iii. Progressive Jackpot (As per Jackpot above.)

c) Door Openings (any external door, that accesses a critical area, on the Gaming Device). Door switches (discrete inputs to the interface element) are acceptable if their operation does not result in redundant or confusing messaging.

d) Coin or Token-In errors ('i' and 'ii' should be sent as a unique message, if supported by the communication protocol):
   i. Coin or Token jams; and
   ii. Reverse Coins or tokens-in.

e) Bill (Item) Validator Errors ('i' and 'ii' should be sent as a unique message, if supported by the communication protocol):
   i. Stacker Full (if supported); and
   ii. Bill (Item) jam.

f) Gaming Device Low RAM Battery Error;

g) Reel Spin Errors (if applicable with individual reel number identified);

h) Coin or Token-Out Errors ('i' and 'ii' should be sent as a unique messages if supported in the protocol):
   i. hopper jams;
   ii. hopper runaways or extra coins paid out; and
   iii. hopper empties (must be sent as a unique message).

i) Printer Errors (if printer supported):
   i. Printer Empty/Paper Low; and
   ii. Printer Disconnect/Failure.

4.2.3 ***Priority Events***. The following significant events must be conveyed to the MCS where a mechanism must exist for timely notification (it is permissible for the following significant events to be sent to the system as a generic error code, in cases where the game is unable to distinguish the specifics of the event:

a) Loss of Communication with Interface element;
b) Loss of Communication with Gaming Device;
c) Memory corruption of the Interface element, if storing critical information; and
d) RAM corruption of the Gaming Device.

4.3 Meters

4.3.1 ***General Statement***. Metering information is generated on a Gaming Device and collected by the interface element and sent to the MCS via a communication protocol. This information may be either read directly from the Gaming Device or relayed using a delta function. Metering information on the MCS shall be labeled so they can be clearly understood in accordance to their function.

4.3.2 ***Required Meters***. The following metering information must be communicated from the Gaming Device and stored on the system in units equal to the denomination of the gaming device or in dollars and cents:

a) Coin In;
   i. The System shall maintain Paytable Coin-In and theoretical payback percentage information provided by the gaming device for each multi-game or multi-denomination/multi-game.
   ii. The System shall maintain Paytable Coin-In and weighted average theoretical payback percentage information provided by each gaming device which contain paytables with a difference in theoretical payback percentage which exceeds 4 percent between wager categories.

b) Coin Out:

c) Coin-Drop (coins-dropped or total value of all coins, bills and ticket/vouchers dropped);

d) Attendant Paid Jackpots (hand-pays);

e) Attendant Paid Cancelled Credits (if supported on Gaming Device);

f) Physical Coin In

g) Physical Coin Out

h) Bills In (total monetary value of all bills accepted);

i) Ticket/Vouchers Out

j) Machine Paid External Bonus Payout

k) Attendant Paid External Bonus Payout

l) Attendant Paid Progressive Payout

m) Machine Paid Progressive Payout

n) Ticket/Vouchers In (total monetary value of all ticket/vouchers accepted)

NOTE: Please refer to the GLI-11 standards for the electronic accounting meters that are to be maintained by the Gaming Device. While these electronic accounting meters should be communicated directly from the Gaming Device to the MCS, it is acceptable to use secondary MCS calculations where appropriate.

4.3.3 ***Clearing Meters***. An interface element should not have a mechanism whereby an unauthorized user can cause the loss of stored accounting meter information, see also Section 3.1.4 'Information Buffering and Integrity Checking.'

4.4 Reporting Requirements

4.4.1 ***General Statement***. Significant event and metering information is stored on the MCS in a database and accounting reports are subsequently generated by querying the stored information.

4.4.2 ***Required Reports***. Reports will be generated on a schedule determined by the Gaming Commission, which typically consists of daily, monthly, yearly period, and life to date reports generated from stored database information. These reports at minimum will consist of the following:

a) Net Win/Revenue Report for each Gaming Device;
b) RESERVED;
c) Drop Comparison Reports for each medium dropped (examples = coins, bills) with dollar and percent variances for each medium and aggregate for each type;
d) Metered vs. Actual Jackpot comparison Report with the dollar and percent variances for each and aggregate;
e) Theoretical Hold vs. Actual Hold comparison with variances;
f) Significant Event Log for each Gaming Device; and
g) Other Reports, as required by individual jurisdictions.

NOTE: It is acceptable to combine reporting data where appropriate (e.g., revenue, theoretical/actual comparison)

NOTE: For additional revenue reporting requirements when ticket/voucher drop Gaming Devices are interfaced, please see '<u>Ticket/-Validation System Requirements</u>,' section 5.0 of this document.

4.5 Security Requirements

4.5.1 ***Access Control***. The MCS must support either a hierarchical role structure whereby user and password define program or individual menu item access or logon program/device security based strictly on user and password or PIN. In addition, the MCS shall not permit the alteration of any significant log information communicated from the Gaming Device. Additionally, there should be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts.

4.5.2 ***Data Alteration***. The MCS shall not permit the alteration of any accounting or significant event log information that was properly communicated from the Gaming Device without supervised access controls. In the event financial data is changed, an automated audit log must be capable of being produced to document:

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).

4.6 Additional System Features

4.6.1 ***Gaming Device Program Verification Requirements***. If supported, a MCS may provide this redundant functionality to check Gaming Device game software. Although the overhead involved can potentially impede Gaming Device and MCS operation, the following information must be reviewed for validity prior to implementation:

a) Software signature algorithm(s); and
b) Data communications error check algorithm(s).

NOTE: The above standard is subject to review based on jurisdictional regulations and may or may not be required of the MCS.

4.6.2 ***Verification Algorithm Timing***. Verification may be user initiated or triggered by specific significant event(s) on the Gaming Device. To ensure complete coverage verification should be performed after each of the following events:

a) Gaming Device Power Up; and

b) New Gaming Device installed.

NOTE: The above standard is subject to review based on jurisdictional regulations and may or may not be required of the MCS.

4.6.3 FLASH Download Requirements. If supported, a MCS may utilize FLASH technology to update interface element software if all of the following requirements are met:

a) FLASH Download functionality must be, at a minimum, password protected, and should be at a supervisor level. The MCS can continue to locate and verify versions currently running but it cannot load code that is not currently running on the system without user intervention;

b) A audit log must record the time/date of a FLASH download and some provision must be made to associate this log with, which version(s) of code was downloaded, and the user who initiated the download. A separate FLASH Audit Log Report would be ideal; and

c) All modifications to the download executable or flash file(s) must be submitted to GLI for approval. At this time, GLI will perform a FLASH download to the system existing at GLI and verify operation. GLI will then assign signatures to any relevant executable code and flash file(s) that can be verified by a regulator in the field. Additionally, all flash files must be available to a regulator to verify the signature.

NOTE: The above refers to loading of new system executable code only. Other program parameters may be updated as long as the process is securely controlled and subject to audit.

4.6.4 ***<u>Remote Access Requirements</u>***. If supported, a MCS may utilize password controlled remote access to a MCS as long as the following requirements are met:

a) Remote Access User Activity log is maintained depicting logon name, time/date, duration, activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database other than information retrieval using existing functions;
d) No unauthorized access to operating system; and
e) If remote access is to be continuous basis then a network filter (firewall) should be installed to protect access.

NOTE: GLI acknowledges that the MCS manufacturer may, as needed, remotely access the MCS and its associated components for the purpose of product and user support. This feature however, must be optional, by a secure means, to accommodate those jurisdictions that do not permit remote access.

4.6.5 ***<u>Verification of System Software –</u>*** System software components/modules shall be verifiable by a secure means (as defined in 4.5.1 Access Controls) 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/modules from an outside source and is required for all control programs that may affect the integrity of the system. This must be accomplished by being authenticated by a third-party device, which may be embedded within the system software (see NOTE below) or having an interface port for a third-party device to authenticate the media. This integrity check will provide a means for field verification of the system components/modules to identify and validate the programs/files. The test laboratory, prior to system approval, shall approve the integrity check method.

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

4.7 Backups and Recovery

4.7.1 ***General Statement***. The MCS shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the MCS with open support for backups and restoration.

4.7.2 ***Recovery Requirements***. In the event of a catastrophic failure when the MCS cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

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

CHAPTER 5

5.0 TICKET/VOUCHER VALIDATION SYSTEM REQUIREMENTS

5.1 Introduction

5.1.1 ***General Statement***. A ticket/voucher validation system may be entirely integrated into a MCS or exist as an entirely separate entity. Ticket/Voucher validation systems are generally classified into two types: bi-directional ticket/voucher systems that allow Gaming Devices to print and redeem ticket/vouchers (TITO) and ticket/voucher out (TO) only systems that allow Gaming Devices to print ticket/vouchers but do not allow ticket/voucher redemption. This chapter primarily addresses bi-directional ticket/voucher systems. Where ticket/voucher out only systems are utilized, some of the following may not apply.

5.1.2 ***Payment by Ticket/Voucher Printer***. Payment by ticket/voucher printer as a method of credit redemption on a Gaming Device is only permissible when the Gaming Device is linked to an approved validation system or MCS that allows validation of the printed ticket/voucher. Validation information shall come from the validation system or MCS using a secure communication protocol.

5.2 Ticket/Voucher Issuance

5.2.1 ***Ticket/Voucher Information used by the Gaming Device while communicating to a validation system.*** The ticket/voucher validation system must be able to communicate the following ticket/voucher data to the Gaming Device to print on the ticket/voucher.

a) Casino Name/Site Identifier;

b) Indication of an expiration period from date of issuance, or date and time the ticket/voucher will expire (24 hr format which is understood by the local date/time format); if applicable

c) System date and time (24 hr format which is understood by the local date/time format);

d) Ticket/Voucher validation number for the Gaming Device to generate the validation number;

5.2.2 Algorithm for generating ticket/voucher validation numbers or seeds

a) ***System Validation*** – the algorithm or method used by the validation system or MCS to generate the ticket/voucher validation number must guarantee an insignificant percentage of repetitive validation numbers.

b) ***Gaming Device generated validation number (system seed) –*** The validation system must send a unique seed to the Gaming Device upon enrolling the Gaming Device as ticket/voucher printing capable. The system may subsequently send a new seed to the Gaming Device after a ticket/voucher is printed. The algorithm or methods used to determine the seed must guarantee an insignificant percentage of repetitive validation numbers.

5.2.3 System Ticket/Voucher Records

a) The validation system must retrieve the ticket/voucher information correctly based on the secure communication protocol implemented, and store the ticket/voucher information into a database.

b) The ticket/voucher record on the host system must contain at a minimum the following ticket/voucher information:

i. Validation number;

ii. Date and time the Gaming Device printed the ticket/voucher (24 hr format which is understood by the local date/time format);

iii. Type of transaction or other method of differentiating ticket/voucher types (assuming multiple ticket/voucher types are available;

iv. Numeric value of ticket/voucher in dollars and cents;

v. Status of ticket/voucher (i.e. valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.);

vi. Date and time the ticket/voucher will expire (24 hr format which is understood by the local date/time format or expiration period from date of issuance;

vii. Machine number (or Cashier/Change booth location number, if ticket/voucher creation outside the Gaming Device is supported) that identifies where the ticket/voucher was issued from.

5.2.4 ***<u>Ticket/Voucher printing during loss of communication with validation system.</u>***

For validation systems that communicate to an Gaming Device through an SMIB (Smart Machine Interface Board), if any links between the SMIB and the back-end database go down, the SMIB must:

a) Not respond to the validation request from the Gaming and stop ticket/voucher printing, or

b) Prevent the Gaming Device from further ticket/voucher issuance, or

c) Not read or store any further ticket/voucher information generated by the Gaming Device.

NOTE: A maximum of 2 (two) off-line ticket/vouchers directly after loss of communication is acceptable, in cases where the interface element has already been 'seeded' by the system, provided the ticket/voucher issuance information is sent immediately, when communication is reestablished.

NOTE: This section will be re-evaluated and revised once the G2S protocol has been adopted and becomes utilized by the gaming device suppliers

5.3 Ticket/Voucher Redemption

5.3.1 ***Online Ticket/Voucher Redemption***. Ticket/Vouchers can be redeemed at Gaming Device, Cashier/Change booths or other approved Validation Terminals (Kiosks) provided they are enrolled for ticket/voucher validation with a validation system. (See GLI-11 3.34 for Gaming Device ticket/voucher validation requirements).

a) The validation system must process ticket/voucher redemption correctly according to the secure communication protocol implemented;

b) The validation system must update the ticket/voucher status on the database during each phase of the redemption process accordingly. In other words, whenever the ticket/voucher status changes, the system must update the database; Upon each status change, the database must indicate the following information:

i. Date and time of status change;

ii. Ticket/Voucher status;

iii. Ticket/Voucher value;

iv. Machine number or source identification from where the ticket/voucher information came from.

5.3.2 RESERVED

5.3.3 ***Cashier/Change Booth Operation***. All validation terminals shall be user and password controlled. Once presented for redemption, the cashier shall:

a) Scan the bar code via an optical reader or equivalent; or

b) Input the ticket/voucher validation number manually; and

c) May print a validation receipt, after the ticket/voucher is electronically validated, if applicable.

5.3.4 ***Validation Receipt Information***. If applicable, the validation receipt, at a minimum, shall contain the following printed information:

a) Machine number;
b) Validation number;
c) Date and Time paid;
d) Amount; and
e) Cashier/Change Booth identifier.

5.3.5 ***Invalid Ticket/Voucher Notification***. The validation system or MCS must have the ability to identify these occurrences and notify the cashier that one of the following conditions exists:

a) Ticket/Voucher cannot be found on file (stale date, forgery, etc.);
b) Ticket/Voucher has already been paid; or
c) Amount of ticket/voucher differs from amount on file (requirement can be met by display of ticket/voucher amount for confirmation by cashier during the redemption process).

5.3.6 ***Offline Ticket/Voucher Redemption***. If the on-line data system temporarily goes down and validation information cannot be sent to the validation system or MCS, an alternate method of payment must be provided either by the validation system possessing unique features, (e.g., validity checking of ticket/voucher information in conjunction with a local database storage), to identify duplicate ticket/vouchers and prevent fraud by reprinting and redeeming a ticket/voucher that was previously issued by the Gaming Device; or use of an approved alternative method as designated by the regulatory jurisdiction that will accomplish the same.

5.3.7 ***Redemption Terminals (Kiosks)***. Refer to GLI-20 Redemption Terminals for technical standards for these devices.

5.4 Reports

5.4.1 ***<u>Reporting Requirements</u>***. The following reports shall be generated at a minimum and reconciled with all validated/redeemed ticket/vouchers:

a) Ticket/Voucher Issuance Report;
b) Ticket/Voucher Redemption Report;
c) Ticket/Voucher Liability Report;
d) Ticket/Voucher Drop Variance Report
e) RESERVED;
f) Transaction Detail Report must be available from the validation system that shows all ticket/vouchers generated by a Gaming Device and all ticket/vouchers redeemed by the validation terminal or other Gaming Device; and
g) Cashier Report, which is to detail individual ticket/vouchers, the sum of the ticket/vouchers paid by Cashier/Change Booth or Redemption Terminal.

NOTE: The requirements for 'b' & 'd' are waived where two-part ticket/vouchers exist for the Gaming Device where the first part is dispensed as an original ticket/voucher to the patron and the second part remains attached to the printer mechanism as a copy (on a continuous roll) in the Gaming Device.
NOTE: This section will be re-evaluated and revised once the G2S protocol has been adopted and becomes utilized by the gaming device suppliers

5.5 Security

5.5.1 ***<u>Database and Validation Component Security</u>***. Once the validation information is stored in the database, the data may not be altered in any way. The validation system database must be encrypted or password-protected and should possess a non-alterable user audit trail to prevent unauthorized access. Further, the normal operation of any device that holds ticket/voucher information shall not have any options or method that may compromise ticket/voucher information. Any device that holds ticket/voucher information in its memory shall not allow removing of the information unless it has first transferred that information to the database or other secured component(s) of the validation system.

CHAPTER 6

6.0 SYSTEM ENVIRONMENTAL AND SAFETY REQUIREMENTS

6.1 Introduction

6.1.1 ***General Statement***. This chapter shall govern the environmental and safety requirements for all system components submitted for review.

6.2 Hardware and Player Safety

6.2.1 ***General Statement***. Electrical and mechanical parts and design principals of the electronic associated hardware may not subject a player to any physical hazards. The test laboratory shall NOT make any finding with regard to Safety and EMC testing as that is the responsibility of the manufacturer of the goods or those that purchase the goods. Such Safety and EMC testing may be required under separate statute, regulation, law or Act and should be researched, accordingly, by those parties who manufacture or purchase said hardware. The test laboratory shall not test for, be liable for, nor make a finding relating to these matters.

6.3 Environmental Effects on System Integrity

6.3.1 ***Integrity Standard***. The Laboratory will perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. An on-line system shall be able to withstand the following tests, resuming game play without operator intervention:

a) Electro-magnetic Interference. Systems shall not create electronic noise that affects the integrity or fairness of the neighboring associated equipment;

b) Electro-static Interference. Protection against static discharges requires that the system's hardware be earthed in such a way that static discharge energy shall not damage or inhibit the normal operation of the electronics or other components within the System. Systems may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit a capacity to recover and complete any interrupted function without loss or corruption of any control or data information associated with the System. The tests will be conducted with a severity level of up to 27KV air discharge.