STANDARD SERIES

GLI-21:

Client-Server Systems

Version: 2.1

Release Date: May 18, 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 of compliance evidencing the certification to this Standard.

This Page Intentionally Left Blank

Client-Server Systems

GLI-21 Revision 2.1

Date Released: May 18, 2007 V2.1 *Final*
Date Released: February 28, 2007 V2.0 *Released for Comment*
Date Released: February 5, 2007 V1.5 *Released for Internal Comment*
Date Released: June 30, 2006 V1.4 *Released for comment*
Date Released: April 29, 2005 V1.3 *Final*
Date Released: April 11, 2005 V1.2 *Released for second commentary period*
Date Created: December 15, 2004 V1.1 *Released for comment*

REVISION HISTORY

Rev 2.1

1.3.1 Clarified to better outline purpose of technical standards
1.4 Removed note regarding GLI-11 compliance because GLI-21 contains applicable GLI-11 rules
1.5.1 Added missing parenthesis
1.5.1.2 Removed additional reference to 'conventional client terminal'
3.1.3 Added concessions for multi-player games
3.1.3 Expanded ability of CSS to perform handpays in loss of communication scenarios
3.2 Added concession for alternate network in situations of intended redundancy
3.2.1 Clarified to assuage confusion of firewall applicability
3.2.2 Added an exception for predefined number of attempts
3.4.1 Removed reference to protocol being approved for use
4.1.1 Removed reference to point of sale and accounting features
4.3.1 Added concession for SSGS to provide command and control functions
4.3.5 Added exception for SQL statements already resident on the system to be used with secure access
4.3.6 Added 'recommendation' to the virus protection rule
4.5.1 Clarified system failure expectations
4.5.2 Changed 'system' to 'database' to set realistic recovery requirements
4.6.1 Added statement that self-monitoring schemes will be reviewed on a case-by-case basis
4.8.1 Clarified game recall requirements to delineate between the recall responsibilities of the client terminal and the server
4.9.3 Parsed out items (d) & (e) as they do not involve the download data library
4.9.4 Created this section to accommodate an audit log to record activity between the server and the clients
4.10.2 Removed statement regarding key or seed of sufficient length
4.10.2 Addressed incorrect references to 'device's memory' in item (e)
4.10.2 Added 'if applicable' statement
4.10.3 Added reference 'activation' after any references to download
4.10.3 Clarified statement regarding forensic examinations
4.10.3(a) Adjusted rule to add explicit reference to foreground downloading
4.11.2 Added clarification that either the server or the client terminal can hold multi-game metering
5.14.4 Adjusted rule to accommodate CSS functionality
5.14.5 Added exception for control program media that is to be altered
5.16 Added additional statement regarding critical memory residing at the CSS
5.26.1 Fortified note to allow consolidation of coin acceptor error conditions
5.26.2 Added concession for either a stacker full or stacker removed message
5.36 Removed inaccurate references to EGD and replaced with client terminal
6.3 Clarified secondary decision comment to mention random selection process instead of client terminal
6.3 Added concession for other methods of preventing cryptanalytic attacks
6.3.5 Removed reference to reseeding at the start of every game as CSS may share an RNG between many client terminals
6.3.9(a) Added the statement that each RNG rescaling process will be evaluated on a case-by-case basis by the laboratory

6.10.9 Updated meter section to clarify that meter maintenance may take place at the server or the client terminal and changed the rule to be a recommendation.

Rev 2.0

In General:

1. General reversion of the Standard to 2.0.
2. Misc clean up for consistency and readability.
3. Minimized cross-reference to other GLI standards by including applicable sections within GLI-21.

Rev 1.5

In General:

1. Changed all references of Game Download to Client-Server.
2. Added 5.0 CSS Client Terminal Requirements.
3. Added 6.0 Software Requirements.

1.5 Changed definition for Client Server Systems.
1.5.1 Amended definition of Server Based Game System.
1.5.2 Amended definition of System Supported Game System.
3.1.3 Added section regarding loss of communication.
3.4 Added section regarding Wide Area Network Communication.
4.1 Additional clarification to this section.
4.2 Added section regarding multiple servers.
4.3 Added section for Server general operation and security requirements.
4.4 Added section regarding Wireless Ethernet Communication
4.5 Amended Rev. 1.4 Section 4.2.
4.6 Amended Rev. 1.4 Section 4.3.
4.7 Amended Rev. 1.4 Section 4.4.
4.8 Added Server recall requirements.
4.9 Amended download data library requirements.
4.10 Amended Rev. 1.4 Section 4.6.
4.11 Amended Rev. 1.4 Section 4.7
4.12 Amended Rev. 1.4 Section 4.8

Rev 1.4

In General:

Changed all reference from ‘ SBCSS ’ to ‘CSS ’
Changed all reference from ‘Central Server’ to ‘CSS Server’

1.5.1 Added definition of a Client-Server System or CSS
1.5.1.1 Added definition of Server Based Client-Server System (SBCSS)
1.5.1.2 Added definition of System Supported Client-Server System (SSCSS)
2.2 Added reference to GLI-13 for communication protocol submission requirements
3.1.2 Removed reference to ‘unauthorized access’ of communication protocol. Instead kept requirement to prevent tampering of communication protocol. Made Data encryption a strong recommendation and removed DES equivalent standards for data encryption.
3.3.1 Added definition of Remote Access.
3.3.2 Added requirement that Remote Access must have either an automatic or manual log
4.2.2 Clarified recovery requirements by adding statement ‘where applicable’
4.6.2, 4.6.2(a), 4.6.2(b) Added statement for game program verification to cover applicable server side game components.
4.6.2 (b) Added statement for ‘embedded software’ may require demonstration to both lab and jurisdiction.
4.6.2(d) Added requirement for game program verification for SSCSS
4.6.2 (f) Added requirement for when the client terminal must verify the game program.
4.6.3 Added ‘where applicable’ statement and removed statement ‘which may occur at any time’.

4.6.3 (b1) Added 'where applicable' statement and requirement for archiving data 24 hours after game data is uploaded.
4.6.3 (b2) Added the client terminal as method to store the current game data.
4.6.3 Added note that a forensic analysis must be possible.
Glossary changes:

1. Changed definition of a control program
2. Added definition of a 'Program Library'

Rev 1.3

In General: Various grammatical changes were made.
1.6.1 added the reference to the purpose of the On-Site test to reference the configuration of the security.
3.1.2 Further clarified that if the encryption method does not meet the rule, any alternative measures will be reviewed and must be approved by the regulator.
3.2.1 Changed the reference from the CSS requiring a firewall to the 'CSS Server' since that is the only element within the system that should be secure. Previously it may have been interpreted that a firewall would have to be placed between the Client Terminal and an associated system.
3.2.2 Added additional information that is to be recorded by the Firewall Audit Logs as recommended by the Missouri Gaming Commission.
3.3.2 Added additional information that is to be recorded by the activity log for Remote Access as recommended by the Missouri Gaming Commission.
4.2.1 Added a minimum requirement for the system backup scheme to be implemented once every day however, the backup scheme will still be reviewed on a case-by-case basis.
4.4.1(b) Reformatted the 'eg' to better clarify that it is not a requirement for the hashing algorithm to use MD5, this was intended to be an example.
4.4.1(d) Removed the requirement for the system to automatically validate the software installed in the Client Terminals however; the system still must have the ability to perform this task on demand.
4.5.1 The requirement for changes to the Game Program Library was modified to allow for other methods, provided the regulator approves them. The rules still includes the original mandate for the access be controlled by the regulator, which is required to avoid having to receive individual approval for each jurisdiction.
4.5.2(c) Removed the reference to the regulatory level alterations to the Game Program Library based on the changes to 4.5.1.
4.6.2(c) Changed the rule to better clarify the intent that any verification method implemented shall not be commercially available software, unless it is intended to be used as a secondary verification method.
4.6.2(d) Removed the requirement for the Client Terminal to verify the approved components every twenty-four hours since this regulation is redundant considering the control program integrity check requirements as outlined within GLI-11.
4.6.3(b)(1) Clarified that the minimum time limit for storage of the uploaded game data is 24-hours, as this information may be needed to resolve player disputes. In addition, clarified that the information can be maintained in a log or script file.
4.7.2 Changed the section title to refer to CSS's that allow the system to change the paytable and/or denomination on the Client Terminal. Previously it only referred to Multi-Paytable games.
4.7.2(c) Clarified that the game shall maintain the master accounting meters in the lowest denomination for the local currency to accommodate international jurisdictions.
4.7.2(d) Clarified that the paytable/denomination can be changed via the system, provided the client terminal is in an idle state when the change actually takes effect.
4.7.2(e) Added a rule to accommodate the altering of denominations of a client terminal via the CSS Server that would only permit such act when the change will not affect the integrity of crediting or paying the patron (i.e., games with fixed denomination hoppers/coin acceptors)
4.7.3 Clarified that systems that do not require regulator control to clear a Client Terminals RAM must receive conceptual approval from the regulator.
4.8.1 Better clarified that Client Terminals may utilize random values as generated by the CSS Server or the client terminal may function independently of the system.
GLOSSARY: Added additional References and Definitions.

Rev 1.1 → 1.2

The revisions from V1.1 and this release are too numerous and there were many regulations that were moved to another area, possibly embedded within a separate rule or omitted completely. It is our belief that giving the details of the changes would be confusing and not effective, although, we have added a summary of the changes that have occurred:
Clarified the intent of this regulation where the CSS Server downloads game programs, Random Values (with the exception of random outcomes), and/or any other Game Content that is received by the Client Terminal for the purpose of the Client Terminal to complete the game play operation. This change eliminates the method of using the 'thin client' technology, which will be addressed within a separate standard upon completion of GLI-21. In general:

- Updated requirements for Backup of systems;
- Further defined Software Verification requirements;
- Added ability of dual control of administrator access;
- Addressed the Regulatory Control game configurations for CSS 's;
- Added support for operator access to install new games, followed with regulator approval; and
- Added further clarifications to the Remote Access requirements.

Table of Contents

CHAPTER 1

1.0 OVERVIEW - STANDARDS FOR CLIENT-SERVER SYSTEMS (CSS)

1.1 Introduction

1.1.1 General Statement. **Gaming Laboratories International, Inc. (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for technical standards without creating their own standards. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 21*, will set forth the technical Standards for Client-Server Systems CSS.

1.1.2 Document History. This document is an essay from many standards documents from around the world. Some GLI has written; some, such as the Australian and New Zealand National Standard and the Nevada Gaming and Control Board were written by Industry Regulators with input from Test Laboratories and machine manufacturers. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual standard. We have listed below, and give credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **Gaming Laboratories International, Inc.** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed FREE OF CHARGE to all those who request it. This standard and all others may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

Gaming Laboratories International, Inc.
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 ***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 Queensland Office of Gaming Regulation;
b) The Tasmanian Department of Treasury and Finance, Revenue and Gaming Division;
c) The ACT Office of Financial Management;
d) The New South Wales Department of Gaming and Racing;
e) The New Zealand Casino Control Authority;
f) The New Zealand Department of Internal Affairs, Gaming Racing & Censorship Division;
g) The Northern Territory Racing and Gaming Authority;
h) The South Australian Office of the Liquor and Gaming Commissioner;
i) The Victorian Casino and Gaming Authority;
j) The Western Australian Office of Racing Gaming and Liquor;
k) The South African Bureau of Standards; and
l) The Nevada Gaming and Control Board.

1.3 Purpose of Technical Standards

1.3.1 ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analysing and certifying Client Terminal game operation.
b) To only test those criteria that impact the credibility and integrity of client terminal gaming from both the Revenue Collection and Player's play point of view.
c) To create a standard that will ensure that the server-based and server-supported games 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 own 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 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.

1.3.2 No Limitation of Technology. 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 Other Documents That May Apply

1.4.1 General Statement. Please refer to our website at www.gaminglabs.com for a complete list of other GLI Standards available, which may also apply.

1.5 Defining Client-Server Systems

1.5.1 ***General Statement***. A Client-Server System (CSS) can be fragmentally defined as either a Server Based Game System (SBGS) or a Server Supported Game System (SSGS). Both of which can be defined as the combination of a Central Server, Client Terminals and all Interface Elements that function collectively for the purpose of linking the client terminal with the Central Server to perform a myriad of functions related to gaming, which may include, but are not limited to:

a) Downloading of Game Logic to the Client Terminals;
b) Central Server Random Number Generation;
c) Thin Client Gaming Configurations.

The communication network may be totally contained within a single venue (LAN) or over a wide area network (WAN) whereby a server in one location supports client terminals in multiple sites.

1.5.1.1 Server Based Game System (SBGS) defined. The combination of a server and client terminals in which the entire or integral portion of game content resides on the server. This system works collectively in a fashion in which the client terminal will not be capable of functioning when disconnected from the system.

1.5.1.2 Server Supported Game System (SSGS) Defined. The combination of a server and client terminal(s) which together allow the transfer of the entire control program and game content to the client terminal(s) for the purpose of downloading control programs and other software resources to the client terminal on an intermittent basis. The client terminals connected to the system are capable of operating independently from the system once the downloading process has been completed. This configuration encompasses cases where the system may take control of peripheral devices or associated equipment typically considered part of a conventional client terminal such as a bill validator or a printer. In a System Supported Game, game outcome is determined by the client terminals connected to the system and not by the system itself. The client terminal is capable of functioning if disconnected from the system.

1.6 Phases of Testing

1.6.1 ***General Statement***. CSS submissions to the Test Laboratory will be performed in two phases:

a) Within the laboratory setting; and
b) On-site following the initial install of the system to ensure proper configuration of the security applications.

NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.

This Page Intentionally Left Blank

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 Refer to GLI-11 for applicable CSS Client Terminal Submission Requirements

2.2 Refer to GLI-13 for CSS Server, Interface Element and Communication Protocol Submission Requirements

This Page Intentionally Left Blank

CHAPTER 3

3.0 COMMUNICATION REQUIREMENTS

3.1 Introduction

3.1.1 General Statement. This chapter refers to communications between the CSS Server(s), all Interface Elements and the Client Terminals used in the CSS environment.

3.1.2 Communication Protocol. Each component of a CSS must function as indicated by the communication protocol implemented. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms, which are designed to prevent tampering. GLI strongly recommends encryption with secure seeds or algorithms. Any alternative measures will be reviewed on a case-by-case basis, with regulator approval.

3.1.3 Loss of Communications. For a Server Based Game System (SBGS), a client must be rendered unplayable if communications from the server or system portion of the client terminal is lost. If a game is in progress, a mechanism must be provided to recover to the point of the game when communications was lost. Alternatively, in a multi-player environment, a loss of communication can result in aborting the game and refunding player's wagers.

In the case of Client Terminals that have lost communications with the server, the CSS must provide a means, such as a hand pay, for patrons to cash out credits indicated on the Server Based client terminal at the time communication was lost.

3.2 System Security

3.2.1 General Statement. In the event the CSS Server is utilized in conjunction with other networks, 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. If an alternate network path exists for redundancy purposes, it must also pass through at least one application-level firewall.

NOTE: Each CSS as submitted to the Test Laboratory will be examined thoroughly to ensure that the proposed field configuration is secure. The Test Laboratory may provide additional security recommendations within the final certification and on-site training to the regulators, if requested.

3.2.2 Firewall Audit Logs. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

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.

♠ *Please 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.*

3.3 Remote Access

3.3.1 General Statement. Remote Access is defined as any access to the system outside of the 'Trusted' Network. Remote Access, where permitted, shall authenticate all computer systems based on the authorized settings of the CSS or firewall application that establishes a connection with the CSS. The security of Remote Access will be reviewed on a case-by-case basis, in conjunction with the current technology and approval from the local regulatory agency. The following are additional requirements:

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.

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

3.3.2 Remote Access Auditing. The CSS Server must maintain an activity log either automatically or have the ability to manually enter the logs depicting all Remote Access information that includes the:

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.

3.4 Wide Area Network Communications

3.4.1 General Statement. Wide Area Network (WAN) communications within the CSS is permitted provided that:

a) the Jurisdiction(s) within which the CSS is to operate do not specifically prohibit the linking of multiple sites;
b) the communications over the WAN are secured from intrusion, interference and eavesdropping via techniques such as use of a Virtual Private Network (VPN), encryption, authentication etc; and
c) only functions documented in the communications protocol are used over the WAN. The protocol shall be provided to the Testing Laboratory. The protocol documentation may be in multiple parts e.g. delivery mechanism and message formats, etc.

This Page Intentionally Left Blank

CHAPTER 4

4.0 CSS SERVER REQUIREMENTS

4.1 Introduction

4.1.1 General Statement. This section covers the elements common to the "back of the house" operations of a CSS. The Game Server(s) may be located locally, within a single facility or may be remotely located outside of the facility such as over a Wide Area Network (WAN). In the case where a CSS Server also performs tasks as required by other systems, (i.e. On-Line Monitoring and Control System, Ticket Validation System, etc) those portions do not apply to the GLI-21 document and would have to be evaluated against the appropriate standard.

4.2 Multiple Servers

4.2.1 General Statement. A CSS may in fact be a collection of servers for load balancing, redundancy or functionality reasons. For example, there might be two or more game servers, a finance server, monitoring server, download server, etc. The system as a whole, which may be a collection of such servers, must meet the full requirements of this specification but not necessarily each server.

4.3 General Operation & Server Security

4.3.1 General Statement. For a Server Based Game System, the Game Server shall generate and transmit to the Client Terminals control, configuration and information data, depending upon the actual implementation, examples are:

a) credit movement,
b) random numbers,
c) game result components, e.g. balls, cards or reel stop positions,
d) actual game results or
e) updates to the credit meter for winning games.

For a System Supported Game System, the Game Server will not participate in the game determination process i.e. the primary functions will be that of downloading control programs and other software resources, or providing command and control instruction that may change the configuration of the of the software already loaded on the client terminal, on an intermittent basis.

4.3.2 ***Security***. The Servers shall be housed in a secure computer room or secure locked cabinet outside of the Player Terminals.

4.3.3 ***Intrusion Protection***. All servers shall have sufficient physical / logical intrusion protection against unauthorized access. Ideally, the system should require Manufacturer and Regulatory Authority providing joint but not separate access.

4.3.4 ***Configuration Access Requirements***. The CSS interface element setup/configuration menu(s) must not be available unless using an authorized access method that is secure.

4.3.5 ***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 a Network Administrators to perform authorized network infrastructure maintenance with the sufficient access rights, that would include the use of SQL statements that were already resident on the system.

4.3.6 ***Virus Protection***. It is recommended all servers and client devices should have adequate virus protection, where applicable.

4.3.7 ***Copy Protection***. Copy protection to prevent unauthorized proliferation or modification of software, for servers or clients, 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; and
b) any device(s) involved in enforcing the copy protection can be individually verified by the methodology described in Section 4.7.2.

4.4 Wireless Ethernet Communication

4.4.1 General Statement. Should a wireless Ethernet communication solution be utilized, it must meet the GLI-26 Standard 'Wireless Gaming Systems'

4.5 System Failure

4.5.1 General Statement. The CSS shall be designed to protect the integrity of pertinent data in the event of a failure. Audit logs, system databases, and any other pertinent data must be stored using reasonable protection methods. If hard disk drives are used as storage media, data integrity must be assured in the event of a disk failure. Acceptable methods include, but are not limited to, multiple hard drives in an acceptable RAID configuration, or mirroring data over two or more hard drives. The method used must also provide open support for backups and restoration. Backup scheme implementation must occur at least once every day, although all methods will be reviewed on a case-by-case basis by the testing laboratory.

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

a) Significant events.
b) Auditing information.
c) Specific site information such as game configuration, security accounts, etc.

4.6 Self Monitoring

4.6.1 General Statement. The CSS must implement self-monitoring of all critical Interface Elements (e.g. Central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of the condition, provided the condition is not catastrophic. The CSS shall be able to perform this operation with a frequency of at least once in every 24-hour period. The implementation of self-monitoring schemes will be reviewed on a case-by-case basis by the testing laboratory. Additionally, all critical interface elements will be reviewed on a case per case basis and may require further action by the system depending upon the severity of the failure.

4.7 CSS Software Verification

4.7.1 ***General Statement***. Each component of the CSS must have a method to be verified via a third-party verification procedure. In addition, the CSS shall have the ability to:

a) Authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or operation, which reside on the medium.
b) Employ a third-party industry standard secure hashing algorithm. (eg. MD5 or SHA1) The algorithm shall use a key or seed of sufficient length and complexity. The manufacturer should be prepared to demonstrate the algorithm choice to both the testing laboratory and jurisdiction.
c) The third-party verification process shall not include any process or security software provided by the operating system manufacturer. A secondary check may use commercially available software by the operating system manufacturer as part of the secondary verification.
d) The CSS Server must be capable of verifying that all control programs are authentic copies of approved games.

4.7.2 ***Verification of devices that cannot be interrogated.*** Program devices that cannot be interrogated, such as Smart cards, may be used provided they are able to be verified by the following methodology:

a) A challenge is sent by the peer device, such as a hashing seed, to which the device must respond with a checksum of its entire program space using the challenge value.
b) The challenge mechanism and means of loading the software into the device is verified by the Testing Laboratory and approved by the regulator.

Such devices, where examination of the source code by the test lab shows that there can be no affect on approved game or monetary outcome, shall not be subject to these requirements.

4.8 Server Recall Requirements

4.8.1 General Statement. The Server that supports a Server Based Game must be able to provide the following information display

a) a complete play history for the most recent game played and at least nine (9) games prior to the most recent game for each client station connected to the Server Based game. The display must indicate the game outcome (or a representative equivalent), intermediate play steps (such as hold and draw sequence or a double-down sequence), credits available, bets placed, credits or coins paid, and credits cashed out. Client Terminals offering games with a variable number of intermediate play steps per game may satisfy this requirement by providing the capability to display the last 50 play steps. The capability to initiate game recall must be available at the client, for recall information specifically associated with the particular client station initiating the game recall. The capacity to initiate game recall for any and all clients that make up the Server Based Gaming System must be available from the system or server portion of the SBGS. The requirement to display game recall applies to all game programs currently installed on the server portion of the Server Based Game.

b) a complete transaction history for transactions with a cashless wagering system to include the most recent and the previous thirty-four transactions prior to the most recent transaction for each client station that incremented any of the cashless in-or out meters. The capability to initiate transaction history must be available at the client terminal for the transaction history specifically associated with the particular client terminal initiating the history information request.

4.9 Download Data Library

4.9.1 General Statement. The Download Data Library refers to the formal storage of all approved data files that may be downloaded to Client Terminals including control and game software, peripheral firmware, configuration data, etc.

4.9.2 Update of Download Data Library Where applicable, the CSS Download Data Library shall only be written to, with secure access that is controlled by the regulator, in which case the manufacturer and/or operator will be able to access the Download Data Library, provided that

this access does not permit adding or deleting Download Data Files; or the Download Data Library shall only be written to using a method that is acceptable by the Test Laboratory and the Regulator.

4.9.3 Download Data Library Audit Log. Any changes that are made to the Download Data Library, including the addition, changing or deletion of Game Programs, must be stored in an un-alterable audit log, which shall include:

a) Time and Date of the access and/or event;
b) Log In Name;
c) Download Data Files added, changed, or deleted;

4.9.4 Download Activity Audit Log. Any record of activity between the Server and the Client that involves the downloading of program logic, the adjustment of client settings/configurations, or the activation of previously downloaded program logic, must be stored in an unalterable audit log, which shall include:

a) The Client Terminal(s) which the Game Program was downloaded to and, if applicable, the program it replaced; and
b) The Client Terminal(s) which the Game Program was activated on and the program it replaced; and
c) Changes to the Client Terminal configuration settings/configurations and what the changes were.

4.10 Download of Client Terminal Data Files and Control Programs

4.10.1 General Statement. This chapter will outline the requirements of the CSS when downloading software, games and other configuration data to Client Terminals, if the Server provides the functionality of downloading control programs and other software resources, whether for a Server Based Game System or a System Supported Game System.

4.10.2 Verification of Control Program. The Client Terminal and/or the applicable Server Side critical Game components shall provide the ability to conduct an independent integrity check of the Game Program, from a third-party outside source. The verification program used for the

integrity check may be embedded within the game software[1] or have an interface port that is used to authenticate the media with the verification program that will not permit the alteration of the program (read only) and:

a) The Client Terminal and/or the applicable Server Side Game components shall authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or operation, which reside on the medium.
b) The Client Terminal and/or the applicable Server Side Game components shall employ a third-party industry standard secure hashing algorithm (eg. MD-5 or SHA-1). If embedded, the manufacturer should be prepared to demonstrate the algorithm choice to both the testing laboratory and jurisdiction.
c) The third-party verification process shall not include any process or security software provided by the operating system manufacturer, unless the purpose is to be used as a secondary verification method.
d) In the event of failed authentication the client terminal should immediately enter an Error Condition with the appropriate audio and visual indicator. This error shall require operator intervention.
e) In the event of a failed authentication after the client terminal has been powered up, the Client Terminal should immediately enter an Error Condition with the appropriate audio and visual indicator (if applicable). This error shall require operator intervention. The game shall display specific error information and shall not clear until either the file authenticates properly, following the operator intervention, or the medium is replaced or corrected, and the memory is cleared (if applicable), the game is restarted, and all files authenticate correctly.
f) The client terminal must verify the game program against the server right after the download and prior to allowing the game to become operational for play.

4.10.3 Control Program. This section will detail the minimum technical standards that shall be met, where applicable, when downloading/activating control programs from the CSS Server to the Client Terminal:

1 If the third-party verification tool is embedded within the game program, the Test Laboratory must be supplied with the tools needed to 'extract' the program from the Client Terminal to have the ability to perform forensic examinations should the client or server yield an invalid signature, at the request of the regulator.

a) The Client Terminal and/or the CSS Server must have a method to monitor and report to the MCS all external door access during a foreground program download and/or activation process. If the CSS does not have the ability to monitor the door access during the foreground program download and/or activation process, the Test Laboratory's report shall indicate as such so that Internal Controls can be developed to ensure the security of the Client Terminal's security, primarily with regard to the cash compartments, where applicable.
b) Below are the methods to store the current game data that is pertinent to the individual Client Terminal when updating the Control Program in an SSGS configuration*:
    i. Where applicable, the Game Data is uploaded and securely stored on the CSS Server and is maintained for a minimum of 24-hours and archived after that time; or is maintained in log or script file. If this method is used, the process in downloading the new Control Program to the Client Terminal must ensure that all critical areas of memory are overwritten by a default value; or
    ii. The Game data is maintained at the client terminal ; or
    iii. If the CSS is not capable of meeting the above regulation, Regulatory Control may be required on the CSS Server for new Client Terminal Control Program downloads. In addition, the alternate methods used will be reviewed by the Test Laboratory and the Regulator on a case-by-case basis.

    **Please note it must be possible to perform a forensic analysis of the game which includes viewing the game data at the CSS Server and/or being able to place it back onto another client terminal for examination purposes.*
c) Prior to execution of updated software, the Client Terminal must be in an Idle State for a time frame determined by the regulatory agency and the software is successfully authenticated, as defined within item 4.10.2, Verification of Control Program.

4.11 Control of Client Terminal Configurations

4.11.1 ***General Statement***. Client Terminals used in a CSS environment that have alterable configurations that require Regulatory Control, as outlined within GLI-11, may be waived provided that the rules within this section are met.

4.11.2 Paytable/Denomination Configuration Changes. Client Terminal Control Programs that offer multiple paytables and/or denominations that can be configured via the CSS Server will not require Regulatory Control to change the paytable selected, provided:

a) All paytables that are available meet the local theoretical payback percentage and odds requirements, where applicable;
b) The client terminal and/or CSS Server maintains the Amounts Bet and Amounts Won meters within Critical Memory for each of the paytables that are available;
c) The Client Terminal maintains the Master Accounting meters in dollars and cents or the lowest denomination available for the local currency;
d) The game is in an Idle State when the update occurs; and
e) The change will not cause inaccurate crediting or payment (i.e., games using coin hoppers and coin acceptors with a fixed denomination.)

4.11.3 Client Terminal Critical Memory Clear. The process of clearing memory on the Client Terminals via the CSS must utilize a secure method that would require Regulatory Control. For systems that do not comply with this rule, the regulator must approve the method used. **Note: Clearing of non-RAM critical memory, or other memory, should meet the same requirement as those outlined herein for RAM.**

4.12 Download of Random Values

4.12.1 General Statement. This Chapter governs elements of a CSS that may be utilized for the generation of Random Values, which are subsequently communicated to the Client Terminal's Control Program that is required for the determination of game outcomes. The CSS Server generation of Random Values does not include the generation of game outcomes[2].

4.12.2 Random Number Generator. In the event the CSS has the ability to download Random Values to the Client Terminal, the Random Number Generator shall function in

2 Systems utilizing finite pools of game outcomes (i.e., Electronic Pull-Tab Systems) shall conform to the GLI-14 Finite Scratch Ticket and Pull-Tab Systems, in addition to the standards set forth herein, where applicable.

accordance with the 99% confidence levels, as outlined within the RNG Requirements of GLI-11 section VI.

CHAPTER 5

5.0 CSS Client Terminal REQUIREMENTS

5.1 Introduction

5.1.1 ***General Statement***. This terminal is used by the player to place wagers, play the game(s) on offer and win prizes (when applicable). The Player Terminal may receive game play information from the Game Server, in the case of System Based Game System (SBGS) or make its own determination in the case of a System Supported Game System (SSGS), and then displays the information to the player. Game play and other functionality may be separated in parts, where some components may be generated within or outside the Player Terminal (e.g., Player Terminals that function with a system).

5.2 Physical Security

5.2.1 ***General Statement***. A client terminal shall be robust enough to resist forced illegal entry.

5.3 Machine and Player Safety

5.3.1 ***General Statement***. Electrical and mechanical parts and design principals of the client terminal may not subject a player to any physical hazards. The gaming test laboratory shall NOT make any finding with regard to Safety and Electromagnetic Compatibility (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 devices. The Gaming Test Laboratory shall not test for, be liable for, nor make a finding relating to these matters.

5.4 Environmental Effects on Game Integrity

5.4.1 ***Game 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. This certification applies exclusively to tests conducted using current and retrospective methodology developed by Gaming Laboratories International, Inc. During the course of testing, Gaming Laboratories International, Inc. inspects for marks or symbols indicating that a device has undergone product safety compliance testing. Gaming Laboratories International, Inc. also performs, where possible, a cursory review of submissions and information contained therein related to Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations and Environmental conditions. Electrostatic Discharge Testing is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of Electronic Client terminals. Compliance to any such regulations related to the aforementioned testing is the sole responsibility of the device manufacturer. Gaming Laboratories International, Inc. claims no liability and makes no representations with respect to such non-gaming testing. The actual data showing the tests performed and the excluded tests are available upon written request.

A client terminal shall be able to withstand the following tests, resuming game play without operator intervention:

a) Random Number Generator. The random number generator and random selection process shall be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference;

b) Electro-Static Interference. Protection against static discharges requires that the machine's conductive cabinets 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 client terminal. Client terminals 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 play without loss or corruption of any control or data information associated with the client terminal. The tests will be conducted with a severity level of a minimum of 27KV air discharge.

5.5 Hardware Requirements-Other

5.5.1 ***General Statement***. Each client terminal shall meet the following hardware requirements:

a) Microprocessor Controlled. Be controlled by one (1) or more microprocessors or the equivalent in such a manner that the game outcome is completely controlled by the microprocessor or a mechanical device, as approved in Section 4.3, 'Mechanical and Electro-Mechanical Random Number Generators (RNG) Requirements'; **(This rule shall not apply to Server-Based Game Configurations where the game outcome is determined by the Server)**

b) On/Off Switch. An on/off switch that controls the electrical current shall be located in a place which is readily accessible within the interior of the machine so that power cannot be disconnected from outside of the machine using the on/off switch. The on/off positions of the switch shall be labeled; and

c) Temperature and Humidity. Client terminals can be expected to operate in a variety of extreme environments. In the event that the designed operational parameters of a client terminal are exceeded, the machine, if incapable of continued proper operation, shall perform an orderly shutdown without loss of game status, accounting, and security event data. The manufacturer should supply any documentation if the device has had temperature and humidity testing against any recognized standard.

5.6 Cabinet Wiring

5.6.1 ***General Statement***. The client terminal shall be designed so that power and data cables into and out of the client terminal can be routed so that they are not accessible to the general public. This is for game integrity reasons only, not for health and safety. Security-related wires and cables that are routed into a logic area shall not be able to be easily removed.

5.7 Machine Identification

5.7.1 ***General Statement***. A client terminal shall have a not easily removable, without leaving evidence of tampering, identification badge, permanently affixed to the exterior of the cabinet by the manufacturer, and this badge shall include the following information:

a) The manufacturer;
b) A unique serial number;
c) The client terminal model number; and
d) The date of manufacture in month/year format.

5.8 Tower Light

5.8.1 ***General Statement***. The client terminal shall have a light located conspicuously on top of the client terminal that automatically illuminates when a player has won an amount or is redeeming credits that the machine cannot automatically pay, an error condition has occurred (including 'Door Open'), or a 'Call Attendant' condition has been initiated by the player. For games such as the 'bar-top style', it is permissible for the tower light to be shared among other machines or be substituted by an audible alarm.

5.9 Manipulation of Power Supply

5.9.1 RESERVED

5.9.2 ***Surges***. The machine shall not be adversely affected, other than resets, by surges or dips of ± 20% of the supply voltage.
NOTE: It is acceptable for the equipment to reset provided no damage to the equipment or loss or corruption of data is experienced in the field.

5.9.3 RESERVED

5.10 Diverter and Drop Box Requirements

5.10.1 Diverter. For client terminals that accept coins or tokens, the software shall ensure that the diverter directs coins to the hopper or to the drop box when the hopper is full. The hopper full detector shall be monitored to determine whether a change in diverter status is required. If the state of the detector changes, the diverter shall operate as soon as possible, or within ten (10) games, after the state change, without causing a disruption of coin flow, or creating a coin jam. Hopper-less client terminals shall always divert coins to the drop box.

5.10.2 Drop Box. If the client terminal is equipped to accept coins or tokens, then the following rules shall be met:

a) Each client terminal equipped to accept coins or tokens shall contain a separate slot drop bucket or slot drop box to collect and retain all such slot coins or tokens that are diverted into the drop box;
b) A slot drop bucket shall be housed in a locked compartment separate from any other compartment of the client terminal; and
c) There must be a method to monitor the drop box area, even if manufactured by a different company.

5.11 External Doors/Compartments Requirements

5.11.1 General Requirements.

a) RESERVED;
b) Doors shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet (i.e., doors and their associated hinges shall be capable of withstanding determined illegal efforts to gain access to the inside of the client terminal and shall leave evidence of tampering if an illegal entry is made);
c) The seal between the cabinet and the door of a locked area shall be designed to resist the entry of objects;
d) RESERVED;
e) RESERVED;

f) All external doors shall be locked and monitored by door access sensors, which when opened shall cease game play (with the exception of a Drop box door), disable all acceptance, and enter an error condition, which at a minimum shall illuminate the tower light and send the error condition to the on-line system, if applicable;
g) It shall not be possible to insert a device into the client terminal that will disable a door open sensor when the machine's door is shut without leaving evidence of tampering;
h) RESERVED; and
i) The sensor system shall register a door as being open when the door is moved from its fully closed and locked position.

5.12 The Logic Door and Logic Area

5.12.1 General Statement. The logic area is a separately locked cabinet area (with its own locked door), which houses electronic components that have the potential to significantly influence the operation of the client terminal. There may be more than one (1) such logic area in a client terminal

5.12.2 Electronic Components. Electronic component items that are required to be housed in one (1) or more logic areas are:

a) CPUs and any program storage device that contains software that may affect the integrity of gaming, including but not limited to the game, accounting, system communication, and peripheral firmware devices involved in or which significantly influence the operation and calculation of game play, game display, game result determination, or game accounting, revenue, or security;
b) RESERVED;
c) RESERVED;
d) Communication controller electronics and components housing the communication program storage device
e) RESERVED; and
f) The back-up device shall be kept within a locked Logic Area.

5.12.3 RESERVED

5.13 Coin/Token and Currency Compartments

5.13.1 General Statement. The coin or token and currency compartments shall be locked separately from the main cabinet area. A separate coin/token compartment shall not be required for coins or tokens necessary to pay prizes in a machine that pays prizes through a drop hopper.

5.13.2 Access to Currency

a) Access to the currency storage area is to be secured via separate key locks and shall be fitted with sensors that indicate door open/close or stacker removed.
b) Access to the currency storage area is to be through two (2) levels of locks (the relevant outer door plus one other door or lock) before the receptacle or currency can be removed.

5.14 Storage of Critical Memory

5.14.1 Non-Volatile Memory Requirements. The following are the memory requirements for Client terminals that are not a part of a 'thin client' Game-Download System (A **thin client** is a computer (client) in client-server architecture networks which depends primarily on the central server for processing activities. The word "thin" refers to the small boot image which such clients typically require - perhaps no more than required to connect to a network and start up a dedicated web browser or "Remote Desktop" connection)

a) The Client terminal shall have the ability to retain data for the electronic meters and shall be capable of maintaining the accuracy of all information required for thirty (30) days after power is discontinued from the machine.
b) Persistent storage devices may be used, such as non-volatile RAM, FLASH, disk drive, etc.
c) If the battery back-up is used as an 'off chip' battery source, it shall re-charge itself to its full potential in a maximum of twenty-four (24) hours. The shelf life shall be at least five (5) years;
d) If the battery back-up is not rechargeable, it shall have an operating life of at least seven (7) years; and

e) Random access memory that uses an off-chip back-up power source to retain its contents when the main power is switched off shall have a detection system which will provide a method for software to interpret and act upon a low battery condition; and
f) Clearing non-volatile memory shall require access to the locked logic area.
g) Critical data may be maintained in peripheral devices provided there is an appropriate handshake device to indicate to the peripheral that the data has been safely stored within the CSS.

5.14.2 Function of Memory Reset. Following the initiation of a memory reset procedure (utilizing a certified Memory Clear method), the game program shall execute a routine, which initializes each and every bit in memory to the default state. For games that allow for partial memory clears, the methodology in doing so must be accurate and the game must validate the un-cleared portions of memory. **Note: Clearing of non-RAM critical memory, or other memory, should meet the same requirement as those outlined herein for RAM.**

5.14.3 Default Reel Position or Game Display. The default reel position or game display after a memory reset shall not be the top award on any selectable line. The default game display, upon entering game play mode, shall also not be the top award. This applies to the base game only and not any secondary bonus devices.

5.14.4 Configuration Settings. A change to a configuration setting that causes an obstruction to the electronic accounting meters must be done via a secure means that can be controlled by a regulator.

5.14.5 Program Identification. All program storage devices that are not intended to be altered during the function of the CSS, including ROMs, EPROMs, FLASH ROMs, DVD, CD-ROM, Compact Flash and any other type of program storage devices shall be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices.

5.15 Contents of Critical Memory

5.15.1 General Statement. Critical memory is used to store all data that is considered vital to the continued operation of the client terminal. This includes, but is not limited to:

a) All electronic meters required in 'Electronic Metering within the Client terminal,' Section 6.10 including last bill data and power up and door open metering;
b) Current credits;
c) Client terminal/game configuration data;
d) Information pertaining to the last ten (10) plays with the RNG outcome (including the current game, if incomplete); and
e) Software state (the last normal state, last status or tilt status the client terminal software was in before interruption).

Note: All of the above should be checked for corruption. If values are corrupt, game play should cease and at a minimum display an appropriate correlating error.

5.16 Maintenance of Critical Memory

5.16.1 General Statement. Critical memory storage shall be maintained by a methodology that enables errors to be identified and corrected in most circumstances. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes. **Note: It is acceptable for critical memory storage to be contained on the CSS Server, provided it meets the critical memory requirements outline herein.**

5.16.2 Comprehensive Checks. Comprehensive checks of critical memory shall be made during each client terminal restart (e.g., processor reset). Upon resumption, the integrity of all critical memory shall be checked. It is recommended that critical memory is continuously monitored for corruption or comprehensive checks occur at the start of game play. In addition, it is recommended that a triple redundancy check be implemented. Test methodology shall detect 99.99 percent of all possible failures including but not limited to items defined in section 5.14.1 and at a minimum enable errors to be identified. **Note: It is acceptable for critical memory**

storage to be contained on the CSS Server, provided it meets the critical memory requirements outline herein.

5.16.3 Control Program. The control program (software that operates the client terminal's functions) shall allow for the client terminal to ensure the integrity of all control program components during execution of said components.

5.16.4 Program Storage Devices (PSDs). All PSDs (program storage devices), in the executable address space of a main processor, shall be validated and checked for corruption during the following conditions:

a) Any processor reset; (e.g. power up and soft reset)
b) RESERVED;
c) The first time the files are loaded for use (even if only partially loaded); and
d) RESERVED.

5.17 Unrecoverable Critical Memory

5.17.1 General Statement. An unrecoverable corruption of Critical Memory shall result in a Critical Memory error. The Critical Memory should not be cleared automatically, result in a tilt condition, which identifies the error and causes the client terminal to cease further function. It is recommended that the player's credits be displayed to avoid player disputes. An unrecoverable Critical Memory error shall require a full memory clear performed by an authorized person. **Note: It is acceptable for critical memory storage to be contained on the CSS Server, provided it meets the critical memory requirements outline herein.**

5.18 Program Storage Device Requirements

5.18.1 ***Requirements for Program Storage Devices***. All program storage devices, including ROMs, EPROMs, FLASH ROMs, DVD, CD-ROM, Compact FLASH and any other type of program storage devices shall:

a) for those devices whose code is not downloaded, be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices and shall only be accessible with access to the locked logic compartment;
b) perform an integrity check (authentication) of the Critical Files or Program Code that operate the Player Terminal during:
   i any power-up; and
   ii the first time the files or program code are loaded for use (even if only partially loaded).
c) software may not be executed without being authenticated or is able to be externally verified.

   Note volatile storage and PSD space that is not critical to machine security (e.g. Video or sound ROM) are not required to be validated. Although GLI recommends a method be put in place for the files to be tested for corruption. If any of the video or sound files contain payout amounts or other information needed by the player the files or program storage must have a secure method of verification , see also Software Verification.

d) Excluding software storage media discussed in Section 5.18.3, the program residing in the Player Terminal shall be contained in a storage medium, which cannot be altered through the use of circuitry or programming of the Player Terminal itself.
e) Is housed within a locked logic compartment; and
f) Meets the Software Verification requirements in Section 4.7 of this document.

5.18.2 ***Externally Written Program Storage***. For a Program Storage Device that is written to externally but not within the Player Terminal (i.e. EPROM, CD) the following rules shall be met:

a) CD-ROM specific based Program Storage shall:
   i Not be a re-writeable disk; and

ii The "Session" shall be closed to prevent any further writing.

b) Non-EPROM specific (including CD-ROM) Program Storage shall meet the following rules:

i The Control Program shall authenticate all Critical Files by employing a hashing algorithm which produces a 'Message Digest' output of at least 128 bits at minimum as certified by the test laboratory and agreed upon by the jurisdiction. The Message Digest(s) shall be stored on a memory device (ROM- based or other medium) within the Player Terminal. Message Digests which reside on any internally writeable medium shall be protected by a suitable authentication methodology or encrypted, using a public/private key algorithm, with a minimum of a 512 bit key. However, a 768 bit key is recommended, or an equivalent algorithm with similar security certified by the test laboratory and agreed upon by the jurisdiction.

Note: For international jurisdictions, the minimum values outlined within this section may be substituted for minimum values that would be applicable for that location.

ii The Player Terminal shall authenticate all Critical Files against the stored Message Digest(s) as required in (i) above. In the event of a failed authentication, after the Player Terminal has been powered up, the Player Terminal should immediately enter an error condition with the appropriate tower light signal or audible alarm, and record the details, including time and date of the error in a log. This error shall require operator intervention. The Player Terminal shall display specific error information and shall not clear until either the file authenticates properly, following the operator intervention, or the medium is replaced or corrected, and memory is cleared, the Player Terminal is restarted, and all files authenticate correctly.

Note: the values in (i) and (ii) above will constantly be re-evaluated based on technology advancements and new security methods available.

5.18.3 Writable Program Storage. The program residing in the Player Terminal that is capable of being erased and reprogrammed without being removed from the Player Terminal, bill changer or other equipment or related device shall:

a) meet the download requirements of Section 4.12, "Download of Player Terminal Data Files and Control Programs"; or

b) only write to alterable storage media containing data, files, and programs that are not critical to the basic operation of the Player Terminal, such as marketing information; or
c) notwithstanding the foregoing, such device may write to media containing critical data, files, and programs provided that the CSS Server(s):
    i. Provides a log of all information that is added, deleted, and modified be stored on the media;
    ii. Verifies the validity of all data, files, and programs which reside on the media using the methods listed in section 5.18.2(b) above.
    iii. Contains appropriate security to prevent unauthorized modifications; and
    iv. Does not allow execution of the software being modified, including game play, while the media containing the critical data, files, and programs are being modified. Note background download of software that is to be activated later may be permitted if all other criteria are met.

NOTE: If the program storage does not comply with any of the above requirements and is a Hard Disk, the media is permissible provided a write-protected drive is used. SCSI Devices are preferred, as they provide a write protect jumper which can be sealed in place by the regulating body. Any other type of drive will have the write line cut and verified in the field, and any other means of write protection will be examined on a case-by-case basis.

5.19 RESERVED

5.20 Printed Circuit Board (PCB)

5.20.1 ***PCB Identification Requirements***. Requirements for PCB identification:

a) Each printed circuit board (PCB) shall be identifiable by some sort of name (or number) and revision level;
b) The top assembly revision level of the PCB shall be identifiable (if track cuts and/or patch wires are added to the PCB, then a new revision number or level shall be assigned to the assembly); and

c) Manufacturers shall ensure that circuit board assemblies, used in their client terminals, conform functionally to the documentation and the certified versions of those PCBs that were evaluated and certified by the test laboratory.
d) The Manufacturers name is recommended

5.21 Patch Wires

5.21.1 Documentation of Patch Wires & Track Cuts. All patch wires and track cuts shall be documented, in an appropriate manner, in the relevant service manual and/or service bulletin and shall be submitted to the test laboratory. This does not prohibit required repairs in the field.

5.22 Switches and Jumpers

5.22.1 General Statement. If the game contains 'Switches and Jumpers,' the following rules shall be met:

a) All switches or jumpers shall be fully documented for evaluation by the test laboratory;
b) Hardware switches which may alter the jurisdictional specific configuration settings, paytables, game denomination, or payout percentages in the operation of the client terminal must meet 'Configuration Settings' Section 3.13.4 of this document and must be housed within a logic compartment of the client terminal. This includes top award changes (including progressives), selectable Blackjack settings, or any other option that would affect the payout percentage whether or not that percentage is within legal limits; and
c) RESERVED.

5.23 Mechanical Devices Used for Displaying of Game Outcomes

5.23.1 General Statement. If the game has mechanical or electro-mechanical devices, which are used for displaying game outcomes, the following rules shall be observed:

a) Electro-mechanically controlled display devices (e.g. reels or wheels) shall have a sufficiently closed loop of control so as to enable the software to detect a malfunction, and/or any attempt to interfere with the correct operation of that device. This requirement is designed to ensure that if a reel or wheel is not in the position it is supposed to be in, an error condition will be generated;
b) Mechanical assemblies (e.g., reels or wheels) shall have some mechanism that ensures the correct mounting of the assembly's artwork, if applicable;
c) Displays shall be constructed in such a way that winning symbol combinations match up with pay lines or other indicators; and
d) A mechanical assembly shall be so designed that it is not obstructed by any other components.

5.24 Video Monitor/Touch Screens

General Statement. All video monitor touch screens shall meet the following rules:

a) Touch screens (if applicable) shall be accurate and once calibrated, shall maintain that accuracy for at least the manufacturer's recommended maintenance period;
b) A touch screen (if applicable) should be able to be re-calibrated by venue staff without access to the machine cabinet other than opening the main door; and
c) There shall be no hidden or undocumented buttons/touch points (if applicable) anywhere on the screen, except as provided for by the game rules that affect game play.

5.25 RESERVED

5.26 Coin or Token, Bill Validators and Other Methods of Inserting Monetary Values into the Client terminal

5.26.1 Coin Or Token Acceptors. If the client terminal uses a coin/token acceptor, the acceptor shall accept or reject the coin/token on the basis of metal composition, mass, composite makeup, or equivalent security. In addition, it shall meet the following rules:

a) Credit Acceptance Conditions. Acceptance of any Coins or Tokens for crediting to the credit meter shall only be possible when the client terminal is enabled for play. Other

states, such as error conditions, including door opens, audit mode and game play, shall cause the disabling of the coin acceptor system;

b) Credit Meter Update on Coin/Token Insertion. Each valid coin/token inserted shall register the actual monetary value or the appropriate number of credits received for the denomination being used on the player's credit meter for the current game or bet meter. If registered directly as credits, the conversion rate shall be clearly stated, or be easily ascertainable from the client terminal.

c) Coin/Token Acceptor Security Features/Error Conditions. The coin acceptor shall be designed to prevent the use of cheating methods such as, but not limited to slugging (counterfeit coins), stringing (coin pullback), the insertion of foreign objects and any other manipulation that may be deemed as a cheating technique. Appropriate correlating error conditions should be generated and the coin acceptor should be disabled;

d) Rapidly Fed Coins. The client terminal shall be capable of handling rapidly-fed coins/tokens or piggy backed coins/tokens so that occurrences of cheating are eliminated. Coins traveling too fast that do not register on the players credit meter should be returned to the player;

e) Direction Detectors. The client terminal shall have suitable detectors for determining the direction and the speed of coin/token travel in the receiver. If a coin/token traveling at too slow of a speed or improper direction is detected, the client terminal shall enter an error condition and display an error condition for at least thirty (30) seconds or be cleared by an attendant;

f) Invalid Coins/Tokens. Coins/tokens deemed invalid by the acceptor shall be rejected to the coin tray and shall not be counted as credits;

g) RESERVED

h) Coin Acceptor Error Conditions. Coin acceptors shall have a mechanism to allow software to interpret and act upon the following conditions:
   i. Coin-In Jam
   ii. Coin-Out Jam
   iii. Reverse Coin-In (coin travelling wrong way through acceptor)
   iv. Coin Too Slow

NOTE: It is acceptable to report Coin-in jam, Reverse Coin-in and Coin Too Slow errors as a generic "Coin-In Error" condition provided the client terminal level requirements specified in 6.13.1 are met. Additionally, the error conditions within this section shall also comply with 'Error Conditions', Section 6.13 unless otherwise noted.

5.26.2 Bill Validators. All paper currency acceptance devices shall be able to detect the entry of valid bills, coupons, Ticket/Vouchers, or other approved notes, if applicable, and provide a method to enable the client terminal software to interpret and act appropriately upon a valid or invalid input. The paper currency acceptance device(s) shall be electronically-based and be configured to ensure that they only accept valid bills of legal tender. Bill validators may also accept coupons, Ticket/Vouchers, or other approved notes and must reject all others in a highly accurate manner. Ticket/Vouchers are paper slips that are treated as a unit of currency, which may be redeemed for cash or exchanged for credits on the client terminal. Coupons are paper slips primarily used for promotional purposes, which may be of a cashable or non-cashable value. The bill input system shall be constructed in a manner that protects against vandalism, abuse, or fraudulent activity. In addition, bill acceptance device(s) shall meet the following rules for all acceptable types of medium:

a) Each valid bill, coupon, Ticket/Voucher or other approved note shall register the actual monetary value or the appropriate number of credits received for the denomination being used on the players credit meter.
b) Credit Meter update upon Bill Insertion. Credits shall only be registered when:
   i. The bill or other note has passed the point where it is accepted and stacked; and
   ii. The acceptor has sent the "irrevocably stacked" message to the client terminal.

c) Bill Validator Security Features. Each bill validator shall be designed to prevent the use of cheating methods such as stringing, the insertion of foreign objects and any other manipulation that may be deemed as a cheating technique. A method for detection of counterfeit bills must be implemented.
d) Credit Acceptance Conditions. Acceptance of any Bills, Ticket/Vouchers, Coupons or other approved notes for crediting to the credit meter shall only be possible when the client terminal is enabled for play. Other states, such as error conditions, including door opens, audit mode and game play, shall cause the disabling of the Bill validator system; with the exception of allowing credit acceptance during game play for devices that allow players to place bets on upcoming events (e.g. horse racing wagering.)
e) Bill Validator Error Conditions: Each client terminal and/or bill validator shall have the capability of detecting and displaying (for bill validators, it is acceptable to disable or flash light(s)) the following bill Validator error conditions:
    i. Stacker Full (it is recommended that an explicit "stacker full" error message not be utilized since this may cause a security issue)
    ii. Bill Jams
    iii. Bill Validator Door Open - where a bill validator door is the belly glass door, a door open signal is sufficient
    iv. Stacker Door Open or Stacker Removed
    v. Bill Validator Malfunction not specified above.

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 6.13 unless otherwise noted.

5.26.3 Communications. All bill validators shall communicate to the client terminal using a bi-directional protocol.

5.26.4 Factory Set Bill Validators. If bill validators are designed to be factory set only, it shall not be possible to access or conduct maintenance or adjustments to those bill validators in the field, other than:

a) The selection of desired acceptance for bills, coupons, Ticket/Vouchers, or other approved notes and their limits;

b) Changing of certified EPROMs or downloading of certified software;
c) Adjustment of the tolerance level for accepting bills or notes of varying quality should not be allowed externally to the machine. Adjustments of the tolerance level should only be allowed with adequate levels of security in place. This can be accomplished through lock and key, physical switch settings, or other accepted methods approved on a case-by-case basis;
d) Maintenance, adjustment, and repair per approved factory procedures; or
e) Options that set the direction or orientation of acceptance.

5.26.5 Tokenization. For games that allow tokenization, the game shall receive monetary value from the bill or coin acceptor and post to the player's credit meter the entire amount inserted and not store fractional credits. It is acceptable for the device to store the fractional credits if:

a) the game maintains the credit meter in dollars and cents or
b) the fractional credits are clearly displayed to the player and the game contains a fractional credit removal feature for the player to cashout residuals at will via an approved means;

5.27 Machine Metering of Bill Validator Events

5.27.1 General Statement. A client terminal, which contains a bill validator device, shall either locally or at the CSS Server maintain sufficient electronic metering to be able to report the following:

a) Total monetary value of all items accepted;
b) Total number of all items accepted; and
c) A breakdown of the bills accepted:
   i. For bills, the game shall report the number of bills accepted for each bill denomination;
d) For all other notes (Ticket/Vouchers and Coupons), the game shall have a separate meter that reports the number of items accepted, not including bills.

5.27.2 Bill Validator Recall. A client terminal that uses a bill validator shall retain either

locally or at the CSS Server the information required in 5.27.1 of the last five (5) items accepted by the bill validator (i.e. Currency, Ticket/Vouchers, Coupons, etc.) The bill validator recall log may be combined or maintained separately by item type. If combined, the type of item accepted shall be recorded with the respective timestamp.

5.28 Acceptable Bill Validator Locations

5.28.1 Bill Validator Location. If a client terminal is equipped with a bill validator, it shall be located in a locked area of the client terminal (e.g., require opening of the main door to access), but not in the logic area. Only the bill, Ticket/Voucher insertion area will be accessible by the player.

5.29 RESERVED

5.30 Bill Validator Stacker Requirements

5.30.1 General Statement. Each bill validator shall have a secure stacker and all accepted bills shall be deposited into the secure stacker. The secure stacker is to be attached to the client terminal in such a manner so that it cannot be easily removed by physical force and shall meet the following rules:

a) The bill validator device shall have a 'stacker full' sensor; (it is recommended that an implicit "stacker full" error message not be utilized since this may cause a security issue)
b) There shall be a separate keyed lock to access the stacker area. This keyed lock shall be separate from the main door. In addition, a separate keyed lock shall be required to remove the bills from the stacker; and (e.g. 2 levels of locks, plus the main door are 3 levels of locks)
c) A tower light or alarm shall be activated whenever there is access to the bill door or the stacker has been removed.

5.31 Credit Redemption

5.31.1 Credit Redemption. Available credits may be collected from the client terminal by the player pressing the "COLLECT" button at any time other than during:

a) A game being played;
b) Audit mode;
c) Any door open;
d) Test mode;
e) A Credit Meter or Win Meter incrementation, unless the entire amount is placed on the meters when the collect button is pressed; or
f) An error condition.

5.31.2 Cancel Credit. If credits are collected, and the total credit value is greater than or equal to a specific limit (e.g., Hopper Limit for hopper games, Printer Limit for printer games, etc.), the game shall lock up until the credits have been paid, and the handpay is cleared by an attendant.

5.32 Coin Hoppers

5.32.1 General Statement. If coin hoppers are used, they are to be monitored, in all game states, by the client terminal control program. Coin hoppers must have the ability to identify hopper coin jams, hopper empty and extra coin paid conditions. In addition, coin hoppers shall prohibit manipulation by the insertion of a light source or any foreign object and there shall not be an abnormal payout when exposed to higher levels of electro-static discharge or if power is lost at any time during a payout.

5.32.2 Acceptable Hopper Locations. If a client terminal is equipped with a hopper it shall be located in a locked area of the client terminal, but not in the logic area or the drop box. Access to the hopper shall require at a minimum opening of the main door.

5.32.3 Hopper Error Conditions A client terminal that is equipped with a hopper shall have mechanisms to allow software to interpret and act upon the following conditions:

a) Hopper empty or timed out;

b) Hopper Jam
c) Hopper runaway or extra Coin paid out;

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 6.13 unless otherwise noted.

5.33 Printers

5.33.1 Payment By Ticket/Voucher Printers. If the client terminal has a printer that is used to make payments, the client terminal may pay the player by issuing a printed Ticket/Voucher. If the taxation limit in a taxing jurisdiction is reached on any single play when using a Ticket/Voucher printer, then the Ticket/Voucher must not be able to be redeemed at any place other than through human interaction (not on another machine or at a self-serve kiosk). The printer shall print on a Ticket/Voucher and provide the data to an on-line data system that records the following information regarding each payout Ticket/Voucher printed. The information listed below can be obtained from the client terminal, interface board, the on-line data management system, or another means:

a) RESERVED;
b) Value of credits in local monetary units in numerical form;
c) Time of day the Ticket/Voucher was printed in twenty-four (24) hour format showing hours and minutes – printing of this information is not required, provided that storage of this information is in the database;
d) Date, in any recognized format, indicating the day, month, and year;
e) Client terminal number or machine number;
f) Unique validation number (including a copy of the validation number on the leading edge of the Ticket/Voucher), and
g) Barcode (not required for Ticket/Vouchers that are non-redeemable at a gaming machine).

NOTE: To meet this standard, the client terminal and/or the CSS Server shall either keep a duplicate copy or print only one (1) copy to the player but have the ability to retain the last twenty-five (25) Ticket/Voucher-out information to resolve player disputes. In addition, an

approved system shall be used to validate the payout Ticket/Voucher, and the Ticket/Voucher information on the central system shall be retained at least as long as the Ticket/Voucher is valid at that location. Note: If this information is held locally at the client terminal it must be able to be viewed at the Server-level.

5.33.2 Printer Location. If a client terminal is equipped with a printer, it shall be located in a locked area of the client terminal (e.g., require opening of the main door to access), but not in the logic area or the drop box. This requirement ensures that changing the paper does not require access to the drop (cash) or logic areas.

5.33.3 Printer Error Conditions. A printer shall have mechanisms to allow software to interpret and act upon the following conditions:

a) Out of paper/paper low; - it is permissible for the client terminal to not lock up for these conditions however, there should be a means for the attendant to be alerted.
b) Printer jam/failure; and
c) Printer disconnected – it is permissible for the client terminal to detect this error condition when the game tries to print.

*NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section **4.13** unless otherwise noted.*

5.34 Ticket/Voucher Validation

5.34.1 Payment By Ticket/Voucher Printer. Payment by Ticket/Voucher printer as a method of credit redemption is only permissible when:

a) the client terminal is linked to a computerized 'Ticket/Voucher Validation System', which allows validation of the printed Ticket/Voucher. **The CSS itself may act as a standalone ticket validation system in cases where this is supported, assuming that it meets the standards in this section.** Validation approval or information shall come from the Ticket/Voucher Validation System in order to validate Ticket/Vouchers. Ticket/Vouchers may be validated at any location, as long as it meets the standards in this

section. Provisions must be made if communication is lost, and validation information cannot be sent to the central system, thereby requiring the manufacturer to have an alternate method of payment. The validation system must be able to identify duplicate Ticket/Vouchers to prevent fraud by reprinting and redeeming a Ticket/Voucher that was previously issued by the client terminal; or

b) by use of an approved alternative method that includes the ability to identify duplicate Ticket/Vouchers to prevent fraud by reprinting and redeeming a Ticket/Voucher that was previously issued by the client terminal.

5.35 Ticket/Voucher Information

5.35.1 ***General Statement***. A Ticket/Voucher shall contain the following printed information at a minimum:

a) Casino Name/Site Identifier;
b) Machine Number (or Cashier/Change Booth location number, if Ticket/Voucher creation, outside the Client terminal is supported);
c) Date and Time (24hr format which is understood by the local date/time format);
d) Alpha and numeric dollar amount of the Ticket/Voucher;
e) Ticket/Voucher sequence number;
f) Validation number;
g) Bar code or any machine readable code representing the Validation number;
h) Type of transaction or other method or differentiating Ticket/Voucher types; (assuming multiple Ticket/Voucher types are available) and
i) Indication of an expiration period from date of issue, or date and time the Ticket/Voucher will expire (24hr format which is understood by the local date/time format).

NOTE: Some of this information may also be part of the validation number or barcode.

5.35.2 ***Ticket/Voucher Types***. If Client terminal Ticket/Voucher generation is supported while not connected to the validation system, the Ticket/Voucher system must generate two different types of Ticket/Vouchers at minimum. On-line and off-line types are denoted respectively by Ticket/Voucher generation either when the validation system and client terminal

are properly communicating or the validation system and client terminal is not communicating properly. When a patron cashes out of an Client Terminal that has lost communication with the validation system, the Client Terminal may print an off-line Ticket/Voucher or lock up in a handpay condition where a handpay receipt may be generated. The off-line Ticket/Voucher or handpay receipt must be visually distinct from an on-line Ticket/Voucher either in format or content while still maintaining all information requirements.

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

5.36 Ticket/Voucher Issuance and Redemption

5.36.1 Ticket/Voucher Issuance. A Ticket/Voucher can be generated at a Client Terminal through an internal document printer, at a player's request, by redeeming all credits. Ticket/Vouchers that reflect partial credits may be issued automatically from a Client terminal. Additionally, cashier/change booth issuance is allowed if supported by the validation system.

5.36.2 Online Ticket/Voucher Redemption. Ticket/Vouchers may be inserted in any Client Terminal participating in the validation system provided that no credits are issued to the Client Terminal prior to confirmation of Ticket/Voucher validity. The patron may also redeem a Ticket/Voucher at a cashier/change booth or other approved validation terminal.

5.36.3 Offline Ticket/Voucher Redemption. The offline Ticket/Voucher redemption may be validated as an Internal Control process at the specific client terminal that issued the Ticket/Voucher. A manual handpay may be conducted for the offline Ticket/Voucher value.

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

This Page Intentionally Left Blank

CHAPTER 6

6.0 SOFTWARE REQUIREMENTS

6.1 Introduction

6.1.1 ***General Statement***. This section of the document shall set forth the technical requirements for the Rules of Play of the game.

6.2 Rules of Play

6.2.1 ***Display***.

a) Payglass/Video Display. Payglasses or video displays shall be clearly identified and shall accurately state the rules of the game and the award that will be paid to the player when the player obtains a specific win. The payglasses or video displays shall clearly indicate whether awards are designated in credits, currency, or some other unit. The client terminal shall reflect any change in award value, which may occur in the course of play. This may be accomplished with a digital display in a conspicuous location of the client terminal, and the game must clearly indicate as such. All paytable information should be able to be accessed by a player, prior to them committing to a bet. Payglasses or video displays shall not be certified if the information is inaccurate or may cause confusion. The "reasonable player" standard shall be used for evaluation;
b) Upcoming wins. The game shall not advertise 'upcoming wins,' for example three (3) times pay coming soon;
c) Extended Feature Information. Each game which offers an extended feature (i.e., Free Games, Re-Spins, Bonus Paytable during the next 'x' games, etc.) must display the number of feature games that are remaining, during each game; and
d) Multiple Decks of Cards. Any games, which utilize multiple decks of cards, should alert the player as to the number of card decks in play.
e) Player Choices. When a non-skill game offers the player a choice, the ratio between the pay resulting from the optimal selection and the pay resulting from the worst selection should be less than or equal to 100.5%. For example, if selection A has an expected pay

(i.e. the average expected return from making a selection) of 215.48 credits and selection B has an expected pay of 214.41 credits, the ratio - 215.48/214.41 - results in 1.005 which is equal to 100.5 %. If the ratio is greater than 100.5%, the game must then display additional information so that the player can make an informed decision regarding optimal play.

6.2.2 Information to be displayed. A client terminal shall display, or shall have displayed on the glass; the following information to the player at all times the machine is available for player input:

a) The player's current credit balance;
b) The current bet amount. This is only during the base game or if the player can add to the bet during the game;
c) All possible winning outcomes, or be available as a menu item or on the help menu;
d) Win amounts for each possible winning outcome, or be available as a menu or help screen item;
e) The amount won for the last completed game (until the next game starts or betting options are modified); and
f) The player options selected (e.g., bet amount, lines played) for the last completed game (until the next game starts or a new selection is made).
g) The denomination being played shall be clearly displayed.
h) A disclaimer regarding Malfunctions Void all Pays should also be clearly displayed is recommended.

6.2.3 Multi-Line Games.

a) Each individual line to be played shall be clearly indicated by the client terminal so that the player is in no doubt as to which lines are being bet on; the credits bet per line and
b) The winning payline(s) shall be clearly discernable to the player. (E.g., on a video game it may be accomplished by drawing a line over the symbols on the payline(s) and/or the flashing of winning symbols and line selection box. Where there are wins on multiple lines, each winning payline may be indicated in turn. (This would not apply to mechanical reel slot games).

6.2.4 Game Cycle. A game is considered completed when the final transfer to the player's credit meter takes place (in case of a win), or when all credits wagered are lost. The following are all considered to be part of a single game:

a) Games that trigger a free game feature and any subsequent free games;
b) "Second screen" bonus feature(s);
c) Games with player choice (e.g., Draw Poker or Blackjack);
d) Games where the rules permit wagering of additional credits (e.g., Blackjack insurance or the second part of a two-part Keno game); and
e) Double-up/Gamble features.

6.3 Mechanical and Electro-Mechanical Random Number Generator (RNG) Requirements

6.3.1 Game Selection Process.

a) All Combinations and Outcomes Shall Be Available. Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game;
b) No Near Miss. After selection of the game outcome, the random selection process shall not make a variable secondary decision, which affects the result shown to the player. For instance, the random number generator chooses an outcome that the game will be a loser. The game shall not substitute a particular type of loser to show to the player. This would eliminate the possibility of simulating a 'Near Miss' scenario where the odds of the top award symbol landing on the payline are limited but frequently appear above or below the payline;
c) RESERVED;
d) No Corruption from Associated Equipment. A client terminal shall use appropriate communication protocols to protect the random number generator and random selection process from influence by associated equipment, which may be communicating with the client terminal.

6.3.2 Random Number Generator Requirements. The use of an RNG results in the selection of game symbols or production of game outcomes. The selection shall:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

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

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

6.3.4 Background RNG Activity Requirement. The RNG shall be cycled continuously in the background between games and during game play at a speed that cannot be timed by the player. The test laboratory recognizes that some time during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this

exception shall be kept to a minimum. Other implementations used to diminish the chance of cryptanalytic attacks on the RNG will be reviewed by the laboratory on a case by case basis.

6.3.5 RNG Seeding. The first seed shall be randomly determined by an uncontrolled event. Thereafter, during random intervals 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 games will not synchronize. Other implementations used to diminish the chance of cryptanalytic attacks on the RNG will be reviewed by the laboratory on a case by case basis.

6.3.6 Live Game Correlation. Unless otherwise denoted on the payglass, where the client terminal plays a game that is recognizable to be a simulation of a live casino game such as Poker, Blackjack, Roulette, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of getting any particular number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38; the odds of drawing a specific card or cards in Poker shall be the same as in the live game. For other game types (such as spinning reel games or video spinning reel games), the mathematical probability of a symbol appearing in a position for any game outcome shall be constant.

6.3.7 Card Games. The consequences for games depicting cards being drawn from a deck are the following:

a) At the start of each game/hand, it is recommended that the first hand of cards shall be drawn fairly from a randomly-shuffled deck; the replacement cards shall not be drawn until needed;
b) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted;
c) RESERVED; and
d) As cards are removed from the deck they shall be immediately used as directed by the Rules of the Game (i.e., the cards are not to be discarded due to adaptive behavior by the client terminal).

6.3.8 Ball Drawing Games. The consequences for games depicting balls being drawn from a barrel (e.g., Keno) are as follows:

a) At the start of each game, only balls applicable to the game are to be depicted. For games with bonus features and additional balls that are selected, they should be chosen from the original selection without duplicating an already chosen ball;
b) RESERVED;
c) The barrel shall not be re-mixed except as provided by the rules of the game depicted; and
d) As balls are drawn from the barrel, they shall be immediately used as directed by the Rules of the Game (i.e., the balls are not to be discarded due to adaptive behavior by the client terminal).

6.3.9 Scaling Algorithms.

a) If a random number with a range shorter than that provided by the RNG is required for some purpose within the client terminal, 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. Each case of RNG re-scaling will be reviewed by the test laboratory on a case-by-case basis.
b) If a particular random number selected is outside the range of equal distribution of re-scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

6.3.10 Mechanical Based RNG Games. Mechanical based RNG games are games that use the laws of physics to generate the outcome of the game. All mechanical based RNG games must meet the requirements of this document with the exception of Sections 6.3.4, 6.3.5, and 6.3.9 that dictate the requirements for electronic random number generators. In addition, mechanical based RNG games must meet the following rules:

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

b) The mechanical pieces must be constructed of materials to prevent decomposition of any component over time (e.g., a ball shall not disintegrate);
c) The properties of physical items used to chose the selection shall not be altered; and
d) The player shall not have the ability to physically interact or come into physical contact or manipulate the machine physically with the mechanical portion of the game.

NOTE: The laboratory reserves the right to require replacement parts after a pre-determined amount of time for the game to comply with Rule 6.3.10(b) above. In addition, the device(s) may require periodic inspections to ensure the integrity of the device. Each mechanical based RNG game shall be reviewed on a case-by-case basis.

6.4 Payout Percentages, Odds and Non-Cash Awards

6.4.1 ***Software Requirements for Percentage Payout***. Each game shall theoretically payout a minimum of seventy-five percent (75%) during the expected lifetime of the base game (e.g., the game percentage without any progressives, bonusing systems, merchandise, etc.)

NOTE: The laboratory will provide the minimum and maximum theoretical payout percentage for the base game within the certification report, unless otherwise noted. Additional awards added to a game will require a re-evaluation of the theoretical payout percentage, considering the value of the award and possibly other factors. The laboratory will re-evaluate a game's theoretical payout percentage when requested.

a) Optimum Play Used for Skill Games. Client terminals that may be affected by player skill shall meet the requirement of Section 6.4.1 when using a method of play that will provide the greatest return to the player over a period of continuous play.
b) Minimum Percentage Requirement Met at All Times. The minimum percentage requirement of 75% shall be met at all times. The minimum percentage requirement shall be met when playing at the lowest end of a non-linear paytable (i.e., if a game is continuously played at a minimum bet level for its total game cycle and the theoretical RTP is lower than the minimum percentage, then the game is unacceptable). This example also extends to games such as Keno, whereby the continuous playing of any

spot combination results in a theoretical return to player lower than the minimum percentage.

c) Double-up or Gamble. The Double-up or Gamble options shall have a theoretical return to the player of one hundred percent (100%).

6.4.2 RESERVED

6.4.3 Multiple Percentages. For games that offer multiple percentages, please refer to the 'Configuration Setting' requirements in section 4.11.2 of this document. For games connected by a network, security measures will be reviewed on a case-by-case basis.

6.4.4 Odds. The highest single advertised payout on each client terminal shall occur, statistically, at least once in 50,000,000 games. This does not apply to multiple awards won together on the same game play where the aggregate prize is not advertised. This odds rule shall not apply to games which make it possible for a player to win the highest win, multiple times through the use of free games. This rule does apply to each wager that wins the maximum award. If the highest advertised award can occur within a bonus or free game feature, the odds calculation shall include the odds of obtaining the bonus round including the odds to achieve the top award.

6.4.5 Merchandise Prizes in Lieu of Cash Awards.

a) RESERVED;
b) Limitations (annuities – lump sum or the payment plan) on the prize amount of Merchandise shall be clearly explained to the player on the game that is offering such a prize.
c) Client terminals which are linked to offer the same merchandise prize, shall have the same probability of hitting the winning combination (adjusted for denomination of play and number of coins bet) that will award that prize. See also, GLI-12 Progressive Client terminals in Casinos.

6.5 Bonus Games

6.5.1 ***Bonus Games***.: Games that have an award calculated, occurring from game play within the base game's cycle made upon the completion of a series of random occurrences, (e.g. bonus features, including free games) shall meet the following:

a) The game shall display clearly to the player which game rules apply to the current game state;
b) The game shall clearly display to the player all possible win amounts, multiplier ranges, etc. that can be obtained from bonus play.
c) The game, other than those that occur randomly, shall display to the player sufficient information to indicate the current status towards the triggering of the next bonus game.
d) If the game requires obtaining several events/symbols toward a feature, the number of events/symbols needed to trigger the bonus shall be indicated along with the number of events/symbols collected at any point.
e) The game shall not adjust the likelihood of a bonus occurring, based on the history of prizes obtained in previous games (i.e., games shall not adapt their theoretical return to player based on past payouts);
f) If a game's bonus is triggered after accruing a certain number of events/symbols or combination of events/symbols of a different kind, the probability of obtaining like events/symbols shall not deteriorate as the game progresses (e.g., for identical events/symbols it is not permitted that the last few events/symbols needed are more difficult to obtain than the previous events/symbols of that kind); and
g) The game shall make it clear to the player that they are in this mode to avoid the possibility of the player walking away from the machine not knowing the game is in a bonus mode.
h) Bonus game awards are part of the game cycle with predetermined award values. Bonus play award contributions to the program payout percentage are calculated consistent with awards of the regular game cycle. Specifically, if the cycle for bonus play awards is different from the base game cycle, then the bonus play awards, occurring within the base game's cycle, will be calculated as part of the game's payout; and
i) Pursuant to the rules, the game shall display the rules of play for the bonus game awards, the rewards associated with each bonus play award, and the character combinations that

will result in the specific payouts. For bonus play awards achieved by obtaining specific game results, the progress of the award shall be displayed.

6.6 RESERVED

6.7 Extra Credits Wagered during Bonus Games

6.7.1 General Statement. If a bonus or feature game requires extra credits to be wagered and the game accumulates all winnings (from the trigger and the feature) to a temporary "win" meter (rather than directly to the credit meter), the game shall:

a) Provide a means where winnings on the temporary meter can be bet (via the credit meter) to allow for instances where the player has an insufficient credit meter balance to complete the feature;
b) Transfer all credits on the temporary meter to the credit meter upon completion of the feature;
c) Not exceed the max bet limit, if one is set; and
d) Provide the player an opportunity NOT to participate.

6.8 Mystery Awards

6.8.1 General Statement. It is acceptable for games to offer a 'Mystery Award' (an award that is not specifically called out on the payglass or game screen) however, the game must indicate the maximum amount the player could potentially win. If the minimum amount that could potentially be awarded is not displayed, it will be assumed to be '0'. In addition, both a minimum and maximum amount must be displayed for any Mystery Award if the method to receive the award involves strategy or skill. This would include methods where the value of the paytable is used in order to make decisions that could increase the return to the player (i.e. Video Poker)

6.9 Multiple Games on the Client terminal

6.9.1 Selection of Game For Display.

a) RESERVED.
b) The methodology employed by a player to select and discard a particular game for play on a multi-game client terminal shall be clearly explained to the player on the client terminal, and be easily followed.
c) The client terminal shall be able to clearly inform the player of all games, their rules and/or the paytables before the player must commit to playing them.
d) The player shall at all times be made aware of which game has been selected for play and is being played, as applicable.
e) When multiple games are offered for play, the player shall not be forced to play a game by just selecting a game title, unless the game screen clearly indicates the game selection is unchangeable. If not disclosed, the player shall be able to return to the main menu.
f) It should not be possible to select or start a new game before the current play is completed and all relevant meters have been updated (including features, gamble and other options of the game) unless the action to start a new game terminates the current play in an orderly manner.
g) The set of games offered to the player for selection, or the paytable, can be changed only by a secure certified method or by a secure player initiated request. The rules outlined in 'Configuration Setting' of this document shall govern the critical memory clear control requirements for these types of selections. However, games that keep the previous paytable's (the paytable just turned off) data in memory, a critical memory clear is not required.
h) No changes to the set of games offered to the player for selection (or to the paytable) are permitted while there are credits on the player's credit meter or while a game is in progress, unless changed by a secure player initiated request.

6.10 Electronic Metering within the Client Terminal

6.10.1 RESERVED

6.10.2 Credit Meter Units and Display. The credit meter shall be maintained in credits or cash value (i.e. applicable local currency) and shall at all times indicate all credits or cash available for the player to wager or cashout with the exception of when the player is viewing an informational screen such as a menu or help screen item. This should be displayed to the player unless a tilt condition or malfunction exists.

6.10.3 RESERVED

6.10.4 Tokenization. If the current local currency amount is not an even multiple of the tokenization factor for a game or the credit amount has a fractional value, the credits displayed for that game may be displayed and played as a truncated amount, (i.e., fractional part removed). However, the fractional credit amount shall be made available to the player when the truncated credit balance is zero. The fractional amount is also known as 'Residual Credit,' see also, 'Tokenization–Residual Credits,' Section 6.1.

6.10.5 Credit Meter – Incrementing. The value of every prize (at end of a game) shall be added to the player's credit meter, except for handpays or merchandise, see also 'Merchandise Prizes In Lieu Of Cash Awards,' Section 6.4.5. The credit meter shall also increment with the value of all valid coins, tokens, bills, Ticket/Vouchers, coupons or other approved notes accepted.

6.10.6 Progressives. Progressives awards may be added to the credit meter if either:

a) The credit meter is maintained in the local currency amount format; or
b) The progressive meter is incremented to whole credit amounts; or
c) The progressive prize in local currency amount format is converted properly to credits upon transfer to the player's credit meter in a manner that does not mislead the player (i.e., make unqualified statement "wins meter amount" and then rounds down on conversion or cause accounting imbalances.

   See also, GLI-12 Progressive Client terminals in Casinos.

6.10.7 Collect Meter. There shall be the facility for a collect meter, which will show the number of credits or cash, collected by the player upon a cashout**.** This should be displayed to

the player unless a tilt condition or malfunction exists (the number of credits or cash collected shall be subtracted from the player's credit meter and added to the collect meter). This meter may or may not include handpays.

6.10.8 Software Meter Information Access. The software meter information shall only be accessible by an authorized person and must have the ability to be displayed on demand using a secure means. For each CSS Server and/or the Player Terminals themselves must store and maintain, the following required electronic meters which must also be displayable at the Player Terminal.

6.10.9 Electronic Accounting and Occurrence Meters. Electronic accounting meters shall be at least ten (10) digits in length. These meters shall be maintained in credit units equal to the denomination, or in dollars and cents. If the meter is being used in dollars and cents format, eight (8) digits must be used for the dollar amount and two (2) digits used for the cent amount. Devices configured for multi-denomination play shall display the units in dollars and cents. The meter must roll over to zero upon the next occurrence, any time the meter exceeds ten (10) digits and after 9,999,999,999 has been reached or any other value that is logical. Occurrence meters shall be at least eight (8) digits in length and roll over to zero upon the next occurrence, any time the meter exceeds (8) eight digits and after a maximum of 99,999,999 has been reached or any other value that is logical. Meters shall be labelled so they can be clearly understood in accordance with their function. All client terminals and/or CSS Servers shall be equipped with a device, mechanism or method for retaining the value of all meter information specified in this section (6.10) which must be preserved for a minimum of 72 hours in the event of power loss to the client terminal. For each player terminal, the CSS Server and/or the Client Terminal themselves must store and maintain the following required electronic meters which must also be displayable at the client terminal. The required electronic meters are as follows (accounting meters are designated with an asterisk '*'):

a) Coin In* The client terminal and/or the CSS Server must have a meter that accumulates the total value of all wagers, whether the wagered amount results from the insertion of coins, tokens, currency, deduction from a credit meter or any other means. This meter shall:

i. Not include subsequent wagers of intermediate winnings accumulated during game play sequence such as those acquired from "double up" games;
ii. For multi-game and multi-denomination/multi-game client terminals, provide the information necessary, on a per paytable basis, to calculate a weighted average theoretical payback percentage; and
iii. For client terminals which are considered slot machines and which contain paytables with a difference in theoretical payback percentage which exceeds 4 percent between wager categories, it is recommended the client terminal/CSS Server maintain and display coin in meters and the associated theoretical payback percentage, for each wager category with a different theoretical payback percentage, and calculate a weighted average theoretical payback percentage for that paytable. Please note this rule does not apply to the game of keno or games of skill.

b) Coin Out* The client terminal and/or the CSS Server must have a meter that accumulates the total value of all amounts directly paid by the machine as a result of winning wagers, whether the payout is made from the hopper, to a credit meter or by any other means. This meter will not record amounts awarded as the result of an external bonusing system or a progressive payout;

c) Coin Drop*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of coins or tokens diverted to the drop;

d) Attendant Paid Jackpots*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of credits paid by an attendant resulting from a single winning alignment or combination, the amount of which is not capable of being paid by the client terminal/CSS itself. This does not include progressive amounts or amounts awarded as a result of an external bonusing system. This meter is only to include awards resulting from a specifically identified amount listed in the manufacturer's par sheet;

e) Cancelled Credits*. The client terminal and/or the CSS Server must have a meter that accumulates the total value paid by an attendant resulting from a player initiated cash-out

that exceeds the physical or configured capability of the client terminal/CSS to make the proper payout amount;

f) Physical Coin In*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of coins or tokens inserted into the client terminal;

g) Physical Coin Out*. The client terminal and/or the CSS Server must have a meter that accumulates the value of all coins or tokens physically paid by the client terminal;

h) Bill In*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of currency accepted. Additionally, the machine must have a specific meter for each denomination of currency accepted that records the number of bills accepted of each denomination;

i) Ticket/Voucher Voucher In*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of all slot machine wagering vouchers accepted by the machine; (A.K.A. Ticket-in)

j) Ticket/Voucher Voucher Out*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of all slot machine wagering vouchers and payout receipts issued by the machine; (A.K.A. Ticket-Out)

k) Electronic Funds Transfer In* (EFT In). The client terminal and/or the CSS Server must have a meter that accumulates the total value of cashable credits electronically transferred from an MCS to the client terminal/CSS when using EFT commands in the function of bonusing, promotions or cashless wagering.

l) Cashless Account Transfer In* (AFT In). (A.K.A. WAT In-Wagering Account Transfer In) The client terminal and/or the CSS Server must have a meter that accumulates the total value of cashable credits electronically transferred to the client terminal/CSS from a wagering account by means of an external connection between the client terminal/CSS and a cashless wagering system;

m) Cashless Account Transfer Out* (AFT Out). (A.K.A. WAT Out-Wagering Account Transfer Out) The client terminal and/or the CSS Server must have a meter that accumulates the total value of cashable credits electronically transferred from the client terminal/CSS Server to a wagering account by means of an external connection between the client teminal/CSS and a cashless wagering system;

n) Non-Cashable Electronic Promotion In*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of non-cashable credits electronically transferred to the client terminal/CSS Server from a promotional account by means of an external connection between the client terminal/CSS and a cashless wagering system;

o) Cashable Electronic Promotion In. The client terminal and/or the CSS Server must have a meter that accumulates the total value of cashable credits electronically transferred to the client terminal/CSS Server from a promotional account by means of an external connection between the client terminal/CSS and a cashless wagering system;

p) Non-Cashable Electronic Promotion Out*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of non-cashable credits electronically transferred from the client terminal/CSS to a promotional account by means of an external connection between the machine and a cashless wagering system;

q) Cashable Electronic Promotion Out*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of cashable credits electronically transferred from the client terminal/CSS to a promotional account by means of an external connection between the client terminal/CSS and a cashless wagering system;

r) Coupon Promotion In*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of all coupons accepted by the client terminal;

s) Coupon Promotion Out*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of all coupons issued by the client terminal;

t) Machine Paid External Bonus Payout*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of additional amounts awarded as a result of an external bonusing system and paid by the client terminal/CSS;

u) Attendant Paid External Bonus Payout*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of amounts awarded as a result of an external bonusing system paid by an attendant;

v) Attendant Paid Progressive Payout*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of credits paid by an attendant as a result of progressive awards that are not capable of being paid by the client terminal/CSS;

w) Machine Paid Progressive Payout*. The client terminal and/or the CSS Server must have a meter that accumulates the total value of credits paid as a result of progressive awards paid directly by the client terminal/CSS. This meter does not include awards paid as a result of an external bonusing system; and

x) Games-played. The client terminal and/or the CSS Server must have meters that accumulates the number of games played

i. Since power reset;
ii. Since door close; and
iii. Since game initialization (memory clear).

y) External Doors. The client terminal and/or the CSS Server must have meters that accumulates the number of times the any external cabinet door that allows access to the logic area or currency compartment which was opened since the last memory clear.

aa) Bill validator door. (i.e. stacker door) The client terminal and/or the CSS Server must have a meter that accumulates the number of times the Bill Validator door has been opened since the last memory Clear

bb) Progressive Occurrence. The client terminal and/or the CSS Server must have a meter that accumulates the number of times each progressive meter is activated See also *GLI-12 Progressive Gaming Devices in Casinos*.

6.10.10 Multi-Game Game Specific Meters. In addition to the one set of master Electronic Accounting Meters required above, each individual game available for play shall have the period meters "Credits Bet" and "Credits Won" in either credits or dollars. Even if a 'double up or gamble' game is lost, the initial win amount/credits bet amount shall be recorded in the game specific meters. Alternatively, there can be separate meters that accounts for the double-up or gamble information, see also, Section 6.10.11. Either way, the method of metering must be understood on the screen.

6.10.11 Double Up or Gamble Meters. For each type of Double-up or Gamble feature offered, there shall be sufficient meters to determine the feature's actual return percentage, which should increment accurately every time a Double-up or Gamble play concludes. If the client terminal does not supply accounting for the Double-Up or Gamble information, the feature must not be enabled for use.

6.11 Tokenization – Residual Credits

6.11.1 General Statement. If residual credits exist, the manufacturer may provide a residual credit removal feature or allow a cancel credit or Ticket/Voucher print to remove the residual credits or return the client terminal to normal game play (i.e., leave the residual credits on the player's credit meter for betting). In addition:

a) RESERVED
b) Residual credits bet on the residual credit removal play shall be added to the Coins-In (or Cash In) meter;
c) If the residual credit removal play is won, the value of the win shall either:
    i. Increment the player's credit meter; or
    ii. Be automatically dispensed, and the value of the coin(s) added to the Coins-Out (or Cash Out) meter;
d) All other appropriate client terminal meters (e.g., Hopper Level) shall be appropriately updated;
e) If the residual credit removal play is lost, all residual credits are to be removed from the credit meter;

f) If the residual credits are cancelled rather than wagered, the client terminal shall update the relevant meters (e.g., cancelled credit) and the last play information;
g) The residual credit removal play feature shall return at least seventy-five percent (75%) to the player;
h) The player's current options and/or choices shall be clearly indicated electronically or by video display. These options shall not be misleading;
i) If the residual credit removal play offers the player a choice to complete the game (e.g., select a hidden card), the player shall be also given the option of exiting the residual credit removal mode and returning to the previous mode;
j) It shall not be possible to confuse the residual credit removal play with any other game feature (e.g., Double-up or Gamble);
k) If the residual credit removal play is offered on a multi-game client terminal, the play shall (for meter purposes of each individual game) either be considered to be a part of the game from which the play was invoked, or be treated as a separate game; and
l) The Last Game Recall shall either display the residual credit removal play result or contain sufficient information (e.g., updated meters) to derive the result.

6.12 Communications Protocol

6.12.1 General Statement. For client terminals that are required to communicate with an on-line system, the device must accurately function as indicated by the communication protocol that is implemented. In addition, please refer to the *GLI-13 Standards for On-line Monitoring and Control Systems (MCS) and Validation Systems in Casinos*.

6.13 Error Conditions

6.13.1 General Statement. Client terminals shall be capable of detecting and displaying the following error conditions and illuminate the tower light for each or sound an audible alarm. Error conditions should cause the client terminal to lock up and require attendant intervention except as noted within this section. Error conditions shall be cleared either by an attendant or upon initiation of a new play sequence after the error has cleared except for those denoted by an

"*" which will require further evaluation since deemed as a critical error. Error conditions shall be communicated to an on-line monitoring and control system, if applicable:

COIN ACCEPTOR ERRORS:

a) Coin-in jam;
b) Coin-out jam;
c) Reverse Coin-In (coin travelling wrong way through acceptor)
d) Coin Too Slow

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 5.26 unless otherwise noted.
NOTE: It is acceptable to report Coin-in jam, Reverse Coin-in and Coin Too Slow errors as a generic "Coin-In Error" condition provided the client terminal level requirements specified in 6.13.1 are met.

HOPPER ERRORS

a) Hopper empty or timed out;
b) Hopper Jam
c) Hopper runaway or extra Coin paid out;

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 5.32 unless otherwise noted.

BILL VALIDATOR ERRORS- It is acceptable to disable the validator or flash light(s) for the following bill Validator error conditions:

a) Stacker Full (it is recommended that an implicit "stacker full" error message not be utilized since this may cause a security issue)
b) Bill Jams
c) Bill Validator Door Open - where a bill validator door is the belly glass door, a door open signal is sufficient
d) Stacker Door Open
e) Stacker Removed

f) Bill Validator Malfunction not specified above

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 5.26 unless otherwise noted.

PRINTER ERRORS

a) Out of paper/paper low; - it is permissible for the client terminal to **not** lock up for these conditions however, there should be a means for the attendant to be alerted
b) Printer jam/failure; and
c) Printer disconnected – it is permissible for the client terminal to detect this error condition when the game tries to print.

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 5.33 unless otherwise noted.

DOOR OPEN ERROR CONDITIONS

a) All external doors (i.e. Main, Belly, Top Box);
b) Drop box door;
c) RESERVED;
d) Bill validator door.(i.e. Stacker door)
e) Any other currency storage area that have a door

NOTE: The error conditions within this section shall also comply with 'Error Conditions', Section 6.15 unless otherwise noted.

OTHER ERROR CONDITIONS

a) memory error*; (In the case of this malfunction, the players credits should be displayed to avoid player disputes)
b) Low memory battery, for batteries external to the memory itself or low power source;
c) Program error or authentication mismatch*;
d) Reel spin errors. The specific reel number shall be identified in the error code. This should be detected under the following conditions:

i. A mis-index condition for rotating reels, that affects the outcome of the game:
ii. In the final positioning of the reel, if the position error exceeds one-half of the width of the smallest symbol excluding blanks on the reel strip; and
iii. Microprocessor controlled reels shall be monitored to detect malfunctions such as a reel which is jammed, or is not spinning freely, or any attempt to manipulate their final resting position.

e) Power reset.

6.13.2 Error Conditions Defined. For games that use error codes, a description of client terminal error codes and their meanings shall be affixed inside the client terminal. This does not apply to video-based games; however, video based games shall display meaningful text as to the error conditions.

6.14 Program Interruption & Resumption

6.14.1 Interruption. After a program interruption (e.g., processor reset), the software shall be able to recover to the state it was in immediately prior to the interruption occurring. If a power failure occurs during acceptance of a bill or other note, the bill validator shall give proper credits or return the note, notwithstanding that there may be a small window of time where power may fail and credit may not be given. In this case, the window shall be less than one (1) second.

6.14.2. Restoring Power. If a client terminal is powered down while in an error condition, then upon restoring power, the specific error message shall still be displayed and the client terminal shall remain locked-up. This is unless power down is used as part of the error reset procedure, or if on power up or door closure, the client terminal checks for the error condition and detects that the error is no longer in existence.

6.14.3 Simultaneous Inputs. The program shall not be adversely affected by the simultaneous or sequential activation of the various inputs and outputs, such as 'play buttons', which might, whether intentionally or not, cause malfunctions or invalid results.

6.14.4 Resumption. On program resumption, the following procedures shall be performed as a minimum requirement:

a) Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully;
b) Client terminal control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication may use the checksum; however, it is preferred that the Cyclic Redundancy Check (CRC) calculations are used as a minimum (at least 16 bit). Other test methodologies shall be of a certified type;
c) The integrity of all critical memory shall be checked; and
d) The bill validator device shall perform a self-test at each power up. In the event of a self-test failure, the bill validator shall automatically disable itself (i.e., enter bill reject state) until the error state has been cleared.

6.14.5 Microprocessor Controlled Reels. (e.g., stepper motor reels) shall re-spin automatically to the last valid play-mode result when the play mode is re-entered, and the reel positions have been altered (e.g., the main door is closed, power is restored, audit mode is exited, or an error condition cleared).

6.15 Door Open/Close

6.15.1 Required Door Metering. The software shall be able to detect and possess specific occurrence meters of access as specified in 6.10.9 to the following doors or secures areas:

a) All external doors (i.e. Main, Belly, Top Box);
b) Drop box door;
c) RESERVED; and
d) Bill validator door.(i.e. stacker door)
e) Any other currency storage area that have a door

6.15.2 Door Open Procedures. When the client terminal's main door is opened, the game shall cease play, enter an error condition, display an appropriate error message, disable coin acceptance and bill acceptance, and either sound an alarm or illuminate the tower light or both.

6.15.3 Door Close Procedures. When the client terminal's main door is closed, the game shall return to its original state and display an appropriate error message, until the next game has ended.

6.16 Taxation Reporting Limits

6.16.1 General Statement. The game shall be capable of entering a lock up condition if a single event is in excess of a limit that is required by a taxing jurisdiction.

6.17 Test/Diagnostic Mode (Demo Mode)

6.17.1 General Statement. If the client terminal is in a test, diagnostic or demo mode, any test that incorporates credits entering or leaving the client terminal (e.g., a hopper test) shall be completed on resumption of normal operation. In addition, there shall not be any mode other than normal operation (ready for play) that increments any of the electronic meters. Any credits on the client terminal that were accrued during the test, diagnostic or demo mode shall be automatically cleared before the mode is exited. Specific meters are permissible for these types of modes provided the meters indicate as such.

6.17.2 Entry To Test/Diagnostics Mode. The main cabinet door of the client terminal may automatically place the client terminal in a service or test/diagnostic mode. Test/diagnostics mode may also be entered, via an appropriate instruction, from an attendant during an audit mode access. These modes should not be accessible to the player.

6.17.3 Exiting From Test/Diagnostic Mode. When exiting from test-diagnostic mode, the game shall return to the original state it was in when the test mode was entered.

6.17.4 Test Games. If the device is in a game test mode, the machine shall clearly indicate that it is in a test mode, not normal play.

6.18 Game History Recall

6.18.1 Number Of Last Plays Required. Information on at least the last ten (10) games is to be always retrievable on the operation of a suitable external key-switch, or another secure method that is not available to the player. If the recall information is provided by the CSS server and the link to the CSS server is down, there must be an alternative means of accessing the recall information available at the site.

6.18.2 Last Play Information Required. Last play information shall provide all information required to fully reconstruct the last ten (10) plays. All values shall be displayed; including the initial credits, credits bet, and credits won, payline symbol combinations and credits paid whether the outcome resulted in a win or loss. This information can be represented in graphical or text format. If a progressive was awarded, it is sufficient to indicate the progressive was awarded and not display the value. This information should include the final game outcome, including all player choices and bonus features. In addition, the results of Double-up or Gamble (if applicable).

6.18.3 Bonus Rounds. The ten (10) game recall shall reflect bonus rounds in their entirety. If a bonus round lasts 'x number of events,' each with separate outcomes, each of the 'x events' shall be displayed with its corresponding outcome, regardless if the result is a win or loss. The recall shall also reflect position dependent events if the outcome results in an award. Client terminals offering games with a variable number of intermediate play steps per game may satisfy this requirement by providing the capability to display the last 50 play steps in addition to each base game.

6.19 Software Verification

6.19.1 General Statement. The device shall have the ability to allow for an independent integrity check of the device's software from an outside source and is required for all control programs that may affect the integrity of the game. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game 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 software to identify and validate the program. The test laboratory, prior to device approval, shall approve the integrity check method.

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

Glossary

Reference	Definition
CSS Server	The 'host' computer that is the primary source of the system controls and information.
Control Program	The control program is the software that operates the Client Terminals functions, including the paytable(s) for the game. The Control Program can run independently of the CSS or may require information generated by the system to perform the Client Terminal functions.
Critical Memory	Critical memory is used to store all data that is considered vital to the continued operation of the client terminal.
Firewall	Network security barrier. A firewall is a device that guards the entrance to a private network and keeps out unauthorized or unwanted traffic.
Game Contents	The downloading of any data, with the exception of the Game Program or Random Values.
Game Data	The data stored within non-volatile memory that reflects the accounting and security events that is specific to the individual Client Terminal, which includes: 1) Error Logs. 2) All Drop Meters. 3) Last Game Recall (this should be maintained within the game history in the event there is a player dispute where the suggested problem took place earlier and was not reported until after the update of the new game, text depiction is an acceptable alternative). 4) Bill Recall. 5) Cashless Transaction Logs. 6) Audit Logs for the Client Terminal Game Program transactions.
Game Program	The control program that resides at the CSS server and/or the client terminal
Download Data Library	A Regulator controlled library that resides at the CSS server that contains the complete game program and/or the server side critical components of a game program.
Idle State	The Client Terminal is in an Idle State, including while the game is disabled, when there is no activity on the device, no credits, and no Error Conditions.
Interface Elements	Every point in communication within the CSS which includes, at a minimum, the CSS Server, Client Terminal and any other equipment that is used for the purpose of transmitting data.
Client Terminal	An element within a CSS that is a client terminal. The Client Terminal in a Server-Supported configuration may function independently of the CSS Server upon a successful Control Program update or, requires Game Content, which is produced by the CSS Server, to function as in a Server-Based configuration.
Random Values	Where a Random Number Generator is stored on the CSS Server, and communicates random numbers to the Client Terminal(s) that are required for the Client Terminal to function, where the Client Terminal's Control Program is not independent of the CSS Server.
Regulatory Control	A method used by and is only accessible to the regulator to ensure the security of the CSS.
Server Based Game System (SBGS)	The combination of a server and client terminals in which the entire or integral portion of game content resides on the server. This system works collectively in a fashion in which the client terminal will not be capable of functioning when disconnected from the system.
Server Supported Game System (SSGS)	The combination of a server and client terminal(s) which together allow the transfer of the entire control program and game content to the client terminal(s) for the purpose of downloading control programs and other software resources to the conventional client terminal or client terminal on an intermittent basis. The client terminals connected to the system are capable of operating independently from the system once the downloading process has been completed. This configuration encompasses cases where the system may take control of peripheral devices or associated equipment typically considered part of a conventional client terminal such as a bill validator or a printer. In a System Supported Game, game outcome is determined by the client terminals connected to the system and not by the system itself. The client terminal is capable of functioning if disconnected from the system.