STANDARD SERIES

GLI-21:

Client-Server Systems

Version: 2.2

Release Date: September 6, 2011

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, LLC** 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, LLC will provide a certificate of compliance evidencing the certification to this Standard.

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

CHAPTER 1

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

1.1 Introduction

1.1.1 General Statement. **Gaming Laboratories International, LLC (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, LLC** 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, LLC
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;
l) The Nevada Gaming and Control Board;
m) NIST Special Publication 800-57 *Recommendations for Key Management – Part 2: Best Practices for Key Management Organization;*
n) Nevada Regulatory 14 Technical Standards; and
o) GSA G2S and S2S protocol standards.

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.

NOTE: 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.

CHAPTER 2
2.0 COMMUNICATION REQUIREMENTS

2.1 Introduction

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

2.1.2 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.

2.1.3 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.

2.2 System Security

2.2.1 General Statement. In the event the CSS Server is utilized in conjunction with another network, 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 too must 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.

2.2.2 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.

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.

2.3 Remote Access

2.3.1 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.

2.3.2 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.

2.4 Wide Area Network Communications

2.4.1 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.

CHAPTER 3
3.0 CSS SERVER REQUIREMENTS

3.1 Introduction

3.1.1 ***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.

3.2 Multiple Servers

3.2.1 ***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.

3.3 General Operation & Server Security

3.3.1 ***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.

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

3.3.3 ***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.

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

3.3.5 ***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 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.

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

3.3.7 ***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 3.7.2.

3.4 Wireless Ethernet Communication

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

3.5 System Failure

3.5.1 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.

3.5.2 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.

3.6 Self Monitoring

3.6.1 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.

3.7 CSS Software Verification

3.7.1 Controlled Server Components.

a) ***General Statement.*** Each component of the CSS must have a method to be verified via a third-party verification procedure. The third-party verification process shall not include any process or security software provided by the operating system or manufacturer. A secondary check may use commercially available software by the system manufacturer as part of any secondary verification.

b) ***General Statement.*** The CSS must be capable of verifying that all control programs contained on the server or system portion are authentic copies of approved components both automatically at least once every 24 hours and on demand. The method of validation must provide at least 128 bits of resolution or must be a bit-for-bit comparison and must prevent the execution of any control program component if the component is determined to be invalid. If an error(s) is detected, the system must provide a visual notification of the invalid program. A program component of the verification mechanism must reside on and securely load from non-alterable media. A report shall be available which details the outcome of each automated execution of the validation mechanism and shall identify any invalid program components.

3.7.2 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.

3.7.3 Controlled Client Terminal Components.

a) General Statement. This section will outline the requirements of the CSS when downloading software, games and other configuration data to Client Terminals.
b) Independent Integrity Checks. The CSS shall provide the ability to conduct an independent integrity check of all applicable controlled components residing on the system.
    i. 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.

3.7.4 Verification of Control Program. The CSS shall provide the ability to authenticate all applicable controlled components for which a copy resides on the system on demand and once every 24 hours and:

a) The CSS 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, and for which a copy resides on the system.

b) The CSS 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 of choice to both the testing laboratory and the Commission.

c) A report shall be available that details the verification results for each controlled component verification.

d) In the event of failed authentication the CSS shall deactivate the controlled component in a manner in which the following functions; including, but not limited to, download, install, and configuration of the controlled component to a connected Client Terminal is not possible. The CSS shall also provide a mechanism to provide notification of the authentication failure to the Commission.

3.8 Server Recall Requirements

3.8.1 ***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. 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.

3.9 Download Data Library

3.9.1 ***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.

3.9.2 ***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 new 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.

3.9.3 ***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; and
c) Download Data Files added, changed, or deleted.

3.9.4 ***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.

3.10 Download of Client Terminal Data Files and Control Programs

3.10.1 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.

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

a) The Client Terminal and/or the SSGS Server must have a method to monitor and report to the Slot Monitoring System all external door access during a foreground program download and/or activation process. If the SSGS 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) Prior to execution of updated software, the Client Terminal must be in an Idle State for four minutes and the software successfully authenticated, as defined within the Verification of control program section of the applicable game regulations.

c) Prior to any software being added or removed from a gaming device or client station comprising a part of a system supported game, that would result in the loss or change of mandatory accounting meter information; a complete set of meter information must be successfully communicated to a slot accounting system.

d) It must be possible to perform a forensic analysis of the game which may include viewing the game data at the CSS Server and/or being able to place the game data back onto another client terminal for examination purposes.

3.11 Control of Client Terminal Configurations

3.11.1 General Statement. Client Terminals used in a CSS environment that have alterable configurations that require Regulatory Control, as outlined within GLI-11 Section 1.5, may be waived provided that the rules within this section are met.

3.11.2 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.)

3.11.3 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.

3.12 Download of Random Values

3.12.1 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.
NOTE: Systems utilizing finite pools of game outcomes (i.e. Electronic Pull-Tab Systems) shall conform to GLI-14 Finite Scratch Ticket and Pull-Tab Systems, in addition to the standards set forth herein, where applicable.

3.12.2 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 accordance with the 99% confidence levels, as outlined within the RNG Requirements of GLI-11 Section 3.3.

CHAPTER 4
4.0 CSS CLIENT TERMINAL REQUIREMENTS

4.1 Introduction

4.1.1 ***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). Where applicable, all client terminals must conform to all requirements for Gaming Devices established by the requested jurisdictional authority.

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.