

Part 5317

Monitoring and Control Systems and Validation

Section	
5317.1	Phases of certification
5317.2	Graphical overview
5317.3	No limitation of technology
5317.4	Scope of standard
5317.5	Exceptions to standard
5317.6	Interface element requirements
5317.7	Metering requirements
5317.8	Battery backup requirements
5317.9	Information buffering
5317.10	Comprehensive checks
5317.11	Interface-element requirements for offline ticketing support
5317.12	Address requirements
5317.13	Configuration access requirements
5317.14	Front end controller and data collector requirements
5317.15	Server and database requirements
5317.16	System clock
5317.17	Synchronization feature
5317.18	Database access
5317.19	Jackpot/fill functionality
5317.20	Tax-reporting threshold
5317.21	Jackpot/fill slip information
5317.22	Surveillance/security functionality
5317.23	Gaming device management functionality
5317.24	Accounting functionality
5317.25	Exclusions
5317.26	Communication protocol
5317.27	Significant events
5317.28	Priority events
5317.29	Meters
5317.30	Required meters
5317.31	Clearing meters
5317.32	Required reports
5317.33	Security requirements
5317.34	Verification algorithm timing
5317.35	FLASH download requirements
5317.36	Remote access requirements
5317.37	Verification of system software
5317.38	Backups and recovery
5317.39	Voucher validation system requirements
5317.40	System environmental and safety requirements

§ 5317.1. Phases of certification.

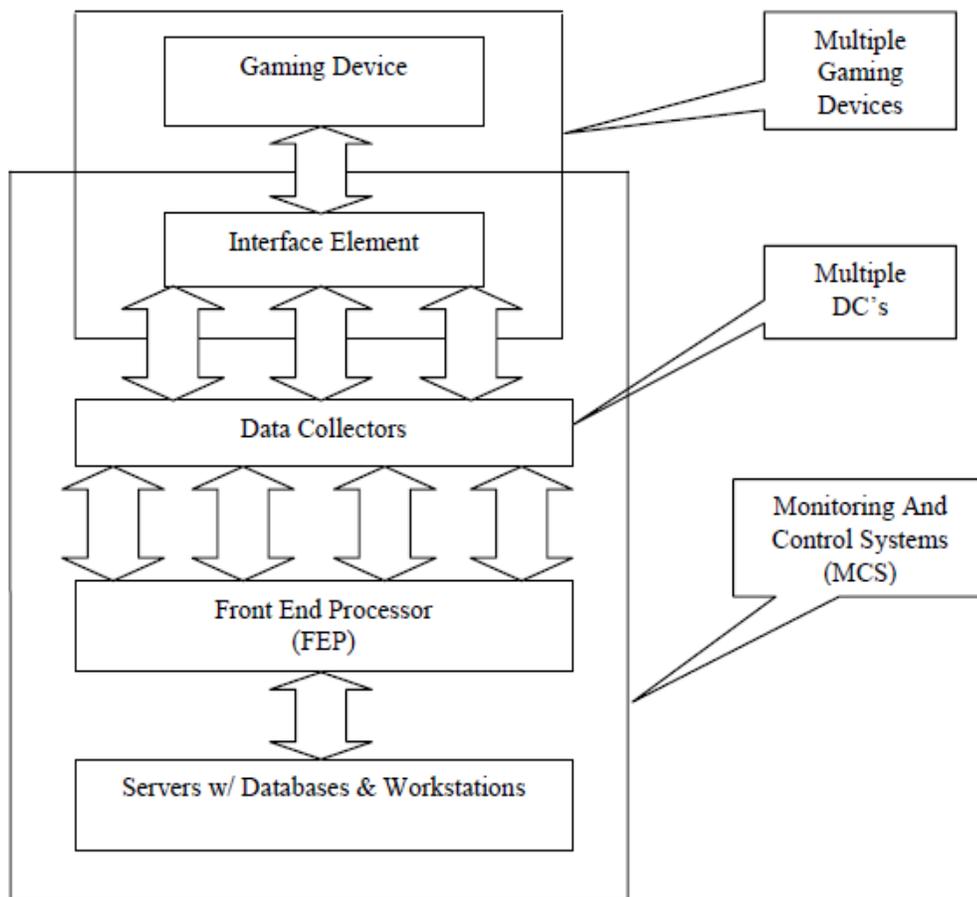
The approval of an online monitoring and control system (*MCS*) shall be certified in two phases:

(a) initial testing, where the licensed independent testing laboratory pursuant to Part 5320 shall test the integrity of the system in conjunction with gaming devices, in a laboratory setting with the equipment assembled; and

(b) onsite certification by a licensed independent testing laboratory pursuant to Part 5318 of this Subchapter, where the communications and setup shall be tested on the gaming facility floor prior to implementation.

§ 5317.2. Graphical overview.

(a) The purpose of this Part is to lend a visual depiction of a generic online monitoring and controls computer system and is not intended to mandate any particular component or system topology, so long as functionality is maintained. The diagram in this subdivision represents the terms used throughout this Part in order to clarify individual components.



(b) This Part is limited to communications from the gaming device to the MCS, and not in the reverse order, with the exception of the voucher validation system requirements that are incorporated in section 5317.40 of this Part.

§ 5317.3. No limitation of technology.

This Part should not be read in such a way that restricts the use of existing technology not mentioned or limits the use of future technology. As new technology is developed, the commission will review this Part and, as necessary, incorporate new minimum standards.

§ 5317.4. Scope of standard.

This Part shall regulate only MCS and validation system requirements necessary to achieve certification when interfaced to gaming devices, for the purpose of mandatory communication of certain security events and electronic meters. All relevant monetary transactions at the gaming-device level shall be handled through:

(a) *Credit issuance.*

- (1) Currency notes (bills) accepted via approved bill validators;
- (2) Approved voucher (items) accepted via approved bill/voucher validators; or
- (3) Player account cards (cashless).

(b) *Credit redemption.*

- (1) Hand-pays;
- (2) Voucher (items) paid by approved voucher printers; or
- (3) Player account cards (cashless).

§ 5317.5. Exceptions to standard.

This Part does not govern MCS requirements for any other form of monetary transaction. Such standard also does not govern advanced bi-directional communication protocols (*i.e.*, EFT, AFT, bonusing, promotional, system-based progressives, features that use an RNG, etc.) that support credit transfer between gaming device and MCS. Such standard supports only one-way communication of events originated at the gaming-device level to the MCS, with the exception of the voucher validation system requirements that are incorporated within section 5317.39 of this Part. Such standard does not exclude gaming devices that operate with player account cashless transactions for the purpose of mandatory communication of security events and electronic meters. All relevant monetary transactions at the slot machine level are handled via electronic transfer through a secure communication protocol.

These device types shall meet the applicable requirements set forth herein, specifically governing metering information and significant events in addition to other commission standards that may apply.

§ 5317.6. Interface element requirements.

Each gaming device installed in a gaming facility shall have a device or interface element installed inside a secure area of such gaming device, that provides for communication between such gaming device and an external data collector.

§ 5317.7. Metering requirements.

If not directly communicating with gaming device meters, an interface element shall maintain separate electronic meters, of sufficient length, to preclude the loss of information from meter rollovers or a means to identify multiple rollovers, as provided for in the connected gaming device. Such electronic meters should be capable of being reviewed on demand, at the interface-element level via an authorized access method.

§ 5317.8. Battery backup requirements.

An interface element shall retain the required information, for no fewer than 72 hours, after a power loss. If this data is stored in volatile RAM, a battery backup shall be installed within the interface element.

§ 5317.9. Information buffering.

If an interface element is unable to communicate the required information to the MCS, such element shall provide a means to preserve all mandatory meter and significant-event information until such time as such information can be communicated to the MCS. Gaming device operation may continue until critical data will be overwritten and lost.

§ 5317.10. Comprehensive checks.

(a) A comprehensive check of interface-element critical memory shall be made during each power resumption and each interface-element restart.

(b) The interface-element critical memory may be monitored continuously for corruption or with comprehensive checks occurring at the start of game play.

(c) The control program (software that operates the interface element's functions) may allow for the interface element to ensure continually the integrity of all control-program components residing in non-volatile memory.

§ 5317.11. Interface-element requirements for offline ticketing support.

The set of minimum requirements set forth in subdivisions (b) through (e) of this section shall be met for an interface element to be capable of providing validation information to

a gaming device for the issuance of offline vouchers after a loss of communication to the voucher validation system has been identified.

(b) The interface element shall be capable of communicating to the game that the offline voucher issuance is supported.

(c) The interface element shall meet the manual authentication identification requirements set forth in subdivision (e) of section 5317.40 of this Part.

(d) The interface element shall limit the number of provided validation numbers and seed, key, etc. values used for the issuance of offline vouchers to a maximum of 25 unused pairs. The interface element shall not provide to a slot machine any more than 25 validation numbers and seed, key, etc. values allowed for the issuance of offline vouchers until all outstanding offline voucher information has been communicated fully to the voucher validation system.

(e) The interface element shall set a maximum expiration length of no more than 30 gaming days for all provided and still unused validation numbers and seed, key, etc. values. Expired validation numbers and seed, key, etc. values shall be discarded in a way that prevents the re-use of unique combinations of validation numbers and seed, key, etc. values for a sufficient period of time on the system.

§ 5317.12. Address requirements.

The interface element shall allow for the association of a unique identification number to be used in conjunction with a gaming device file on the MCS. Such identification number shall be used by the MCS to track all mandatory information of the associated gaming device. Additionally, the MCS should not allow for duplicate gaming device file entry of such identification number.

§ 5317.13. Configuration access requirements.

The interface element setup/configuration menu, or menus, shall be unavailable unless such menus are being used in an authorized access method.

§ 5317.14. Front end controller and data collector requirements.

A MCS may possess a front end processor (*FEP*) that gathers and relays all data from the connected data collectors to the associated database or databases. The data collectors, in turn, collect all data from connected gaming devices. Communication between components shall be via a method approved by the commission and at a minimum conform to the communication protocol requirements set forth in section 5317.27 of this Part. If the FEP maintains buffered/logging information, there shall be a system in place that prevents the loss of critical information contained therein.

§5317.15. Server and database requirements.

A MCS shall consist of a server or servers, networked system or distributed systems that direct overall operation. A MCS shall possess an associated database that stores, or databases that store, all entered and collected system information.

§ 5317.16. System clock.

A MCS shall maintain an internal clock that reflects the current time and date that shall be used to provide for the following:

- (a) time stamping of significant events;
- (b) reference clock for reporting; and
- (c) time stamping of configuration changes.

§ 5317.17. Synchronization feature.

The MCS shall be able to synchronize any clock connected to the MCS.

§ 5317.18. Database access.

The MCS shall not have a built-in facility in which a gaming facility patron or employee can bypass the system auditing to modify the database directly. Gaming facilities shall maintain secure access control.

§ 5317.19. Jackpot/fill functionality.

A MCS system shall have an application or facility that captures and processes every hand-pay message from each gaming device. Hand-pay messages shall be created for single wins (jackpots), progressive jackpots and accumulated credit cashouts (canceled credits), each of which results in hand-pays.

§ 5317.20. Tax-reporting threshold.

Every single-win or hand-pay message received by the MCS that is in excess of a limit that is required by Federal or State tax reporting shall advise the user of the need for a W2-G or 1042-S form to be processed, either via the MCS or manually. This option shall not be capable of being overridden. The keyed reset ability to return winnings from a taxable event to a gaming device should require user intervention to void the original jackpot slip that is generated.

§ 5317.21. Jackpot/fill slip information.

The following information is required for all slips generated by the MCS (subdivisions (b) through (f), (m) and (n) apply to fill slips and subdivisions (b) through (e) and (g) through (n) apply to jackpot slips):

- (a) type of slip;
- (b) numeric slip identifier (which increments per event);
- (c) date and time (shift, if required);
- (d) gaming device number;
- (e) denomination;
- (f) amount of fill;
- (g) amounts of jackpot, accumulated credit and additional pay;
- (h) W-2G indication, if applicable;
- (i) additional payout, if applicable;
- (j) total before taxes and taxes withheld, if applicable;
- (k) amount to patron;
- (l) total credits played and game outcome of award;
- (m) soft meter readings; and
- (n) relevant signatures as required by the commission.

§ 5317.22. Surveillance/security functionality.

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

- (a) date and time range;
- (b) unique interface element/gaming device identification number; or
- (c) significant event number/identifier.

§ 5317.23. Gaming device management functionality.

A MCS shall have a master slot file that is a database of every gaming device in operation at such gaming facility, including, at minimum, the following information for each entry:

- (a) unique interface element/location identification number;
- (b) gaming device identification number as assigned by the gaming facility;
- (c) denomination of the gaming device (such denomination may reflect an alternative value, in the case of a multi-denomination game);
- (d) theoretical hold of the gaming device; and
- (e) control program or programs within the gaming device.

If the MCS retrieves any of such parameters directly from the gaming device, sufficient controls shall be in place to ensure accuracy of such information.

§ 5317.24. Accounting functionality.

A MCS shall have an application or facility that allows controlled access to all accounting (financial) information and shall be able to create all mandatory reports in the reporting requirements under section 5317.32 and any additional reports the commission may require.

§ 5317.25. Exclusions.

Generally, any system or component not specified in this Part that impacts revenue reporting shall be submitted for testing to the independent laboratory approved by the commission pursuant to Part 5320 of this Subchapter. For example, a standalone player-tracking system is not required for submission unless the function of such system includes embedded features that affect revenue. Such systems may be tested for operation and version control if such features are integrated in a MCS submission.

§ 5317.26. Communication protocol.

A monitoring and control system shall support a defined communication protocol and function as indicated by the communication protocols. A MCS shall provide for the following:

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

§ 5317.27. Significant events.

(a) Notice of significant events that a gaming device generates shall be sent via the interface element to the MCS using an approved communication protocol. Each such event shall be stored in a database that includes the following:

- (1) date and time that the event occurred; and
- (2) identity of the gaming device that generated such event; and
 - (i) a unique number/code that defines such event; or
 - (ii) a brief text that describes the event in the local language.

(b) Significant events including the following shall be collected from the gaming device and transmitted to the system for storage:

- (1) power resets or power failure;
- (2) hand-pay conditions (amount needs to be sent to the system):
 - (i) gaming device jackpot (an award in excess of the single-win limit of the gaming device);
 - (ii) cancelled credit hand-pay; and
 - (iii) progressive jackpot (an award in excess of the single-win limit of the gaming device).
- (3) door openings (any door that gives access to a critical area on the gaming device). Door switches (discrete inputs to the interface element) are acceptable if their operation does not result in redundant or confusing messaging;
- (4) bill (item) validator errors (the errors described in subparagraphs (i) and (ii) of this paragraph should be sent as a unique message, if supported by the communication protocol):
 - (i) stacker full (it is recommended that an explicit “stacker full” error message not be used, because doing so may promote a security issue, but “bill validator malfunction” or the equivalent may not); and
 - (ii) bill (item) jam.
- (5) gaming device low RAM battery error;
- (6) reel spin errors (if applicable with individual reel number identified);
- (7) printer errors (if printer supported):

- (i) printer empty/paper low; and
- (ii) printer disconnect/failure.

§ 5317.28. Priority events.

The following significant events shall be conveyed to the MCS in a timely manner in cases where the game is unable to distinguish the specifics of the event:

- (a) loss of communication with interface element;
- (b) loss of communication with gaming device;
- (c) memory corruption of the Interface element, if storing critical information; and
- (d) RAM corruption of the gaming device.

It is permissible for each of the significant events described in paragraphs (a) through (d) of this section to be sent to the system as a generic error code.

§5317.29. Meters.

Metering information shall be generated on a gaming device and collected by the interface element and sent to the MCS via a communication protocol. Such information may be either read directly from the gaming device or relayed using a delta function. Metering information on the MCS shall be labeled so that such information can be understood clearly in accordance with the relevant function.

§ 5317.30. Required meters.

While electronic accounting meters should be communicated directly from the gaming device to the MCS, it is acceptable to use secondary MCS calculations where appropriate. The metering information described in paragraphs (a) through (f) of this section shall be communicated from the gaming device and stored on the system in units equal to the denomination of the gaming device or in dollars and cents.

(a) Coin in.

(1) The system shall maintain pay table coin-in and theoretical payback percentage information provided by the gaming device for each multi-game or multi-denomination/multi-game.

(2) The system shall maintain pay table coin-in and weighted average theoretical payback percentage information provided by each gaming device that contains pay tables with a difference in theoretical payback percentage that exceeds four percent between wager categories.

(3) This subdivision shall not apply to keno or skill games.

- (b) Coin out.
- (c) Total drop (total value of all bills and vouchers dropped).
- (d) Attendant paid jackpots (hand-pays).
- (e) Attendant paid cancelled credits (if supported on the gaming device).
- (f) Bills in (total monetary value of all bills accepted).
- (g) Vouchers out.
- (h) Machine-paid external bonus payout.
- (i) Attendant-paid external bonus payout.
- (j) Attendant-paid progressive payout.
- (k) Machine-paid progressive payout.
- (l) Vouchers in (total monetary value of all vouchers accepted).

§ 5317.31. Clearing meters.

An interface element shall not have a mechanism whereby an unauthorized user can cause the loss of stored accounting meter information. See also section 5317.10 of this Part.

§ 5317.32. Required reports.

Significant event and metering information shall be stored on the MCS in a database and accounting reports are generated subsequently by querying the stored information. Reports shall be generated on a schedule determined by the commission, which typically consists of daily, monthly and yearly periods and life-to-date reports generated from stored database information. Such reports at minimum shall consist of the following:

- (a) net win/revenue report for each gaming device;
- (b) drop comparison reports for each medium dropped (*e.g.*, coupons, bills) with dollar and percent variances for each medium and aggregate for each type;
- (c) metered versus actual jackpot comparison report with the dollar and percent variances for each and aggregate;
- (d) theoretical hold versus actual hold comparison with variances;
- (e) significant event log for each gaming device; and

(f) other reports, as required by the commission.

§ 5317.33. Security requirements.

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

(b) *Data alteration.* The MCS shall not permit the alteration of any accounting or significant-event-log information that was properly communicated from the gaming device without supervised access controls. In the event that financial data is changed, an automated audit log shall be capable of being produced to document:

- (1) data element altered;
- (2) data element value prior to alteration;
- (3) data element value after alteration;
- (4) time and date of the alteration; and
- (5) personnel who performed the alteration (by reporting user login).

(c) *Additional system features; gaming device program verification requirements.* If supported, a MCS may provide redundant functionality to check gaming device game software. The following information shall be reviewed for validity prior to implementation:

- (1) software signature algorithm or algorithms; and
- (2) data communications error-check algorithm or algorithms.

§ 5317.34. Verification algorithm timing.

Verification may be user-initiated or triggered by a specific significant event or events on the gaming device. To ensure complete coverage, verification should be performed after each of the following events:

- (a) gaming device power up; and
- (b) new gaming device installed.

§ 5317.35. Flash download requirements.

If supported, a MCS may use flash technology to update interface element software if all of the following requirements are met:

(a) flash download functionality shall be, at a minimum, password-protected and should be at a supervisor level. The MCS can continue to locate and verify versions currently running, but the MCS is not permitted to load code that is not currently running on the system without user intervention;

(b) an audit log shall record the time and date of a flash download and some provision shall be made to associate such log with the version, or versions, of code that was downloaded and with the user who initiated such download. A separate flash audit log report is recommended; and

(c) all modifications to the download-executable or flash file or files shall be submitted to and licensed independent testing laboratory for approval. Such approved laboratory shall perform a flash download to the system existing at such approved laboratory and verify operation. Such approved laboratory shall then assign signatures to any relevant executable code and flash file or files that can be verified by a commission representative in the field. Additionally, each flash file shall be available to the commission to verify the signature of such file.

Subdivisions (a) through (c) of this section refer to loading of new system-executable code only. Other program parameters may be updated so long as the process is controlled securely and subject to audit.

§ 5317.36. Remote access requirements.

If supported, a MCS may use password-controlled remote access to a MCS so long as the following requirements are met:

(a) remote access user-activity log is maintained depicting logon name, time, date, duration and activity while logged in;

(b) no unauthorized remote-user administration functionality (adding users, changing permissions, etc.) shall be permitted;

(c) no unauthorized access to the database, other than information retrieval using existing functions, shall be permitted;

(d) no unauthorized access to the operating system shall be permitted; and

(e) if remote access is to be continuous, then a network filter (firewall) shall be installed to protect access.

§ 5317.37. Verification of system software.

System software components and modules shall be verifiable by a secure means at the system level, denoting program identification and version. The system shall have the ability to allow for an independent integrity check of the components and modules from an outside source. Such ability is required for all control programs that may affect the integrity of the system. Such ability shall be capable of being authenticated by a third-party device, which may be embedded within the system software or having an interface port for a third-party device to authenticate the media. Such integrity check shall provide a means for field verification of the system components and modules to identify and validate the programs and files. The licensed independent testing laboratory, prior to system approval, shall approve the integrity check method. If the authentication program is contained within the system software, the manufacturer shall receive written approval from the licensed independent testing laboratory prior to submission.

§ 5317.38. Backups and recovery.

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

(b) *Recovery requirements.* In the event of a catastrophic failure when the MCS cannot be restarted in any other way, the system shall have the capability of being reloaded from the last viable backup point and fully recovering the contents of such backup, which should consist of at least the following information:

(1) significant events;

(2) accounting information;

(3) auditing information;

(4) specific site information, such as slot file, employee file, progressive set-up, etc.;

and

(5) If voucher issuance is supported, all information used in the voucher redemption process, including information specific to the redemption of offline vouchers, if applicable.

§ 5317.39. Voucher validation system requirements.

(a) *Voucher validation system.* A voucher validation system may be integrated entirely into a MCS or exist as an entirely separate system.

(b) *Payment by voucher printer.* Payment by voucher printer as a method of credit redemption on a gaming device is permissible only when the gaming device is linked to

an approved validation system or MCS that allows validation of the printed voucher. Validation information shall come from the validation system or MCS using a secure communication protocol. For support of offline voucher issuance, the gaming device shall be linked to an approved validation system or MCS that allows validation of the printed voucher, but does not have to be in constant communication for the issuance of voucher to be permissible.

(c) *Voucher Issuance*. The voucher validation system shall be able to communicate the following voucher data to the gaming device to print on the voucher:

- (1) gaming facility name and site identifier;
- (2) indication of an expiration period from the date of issuance, or the date and time the voucher will expire (24-hour format that is understood by the local date and time format), if applicable;
- (3) system date and time (24-hour format that is understood by the local date and time format); and
- (4) voucher validation number for the gaming device to generate the validation number.

(d) *Algorithm for generating voucher validation numbers or seeds*.

- (1) System validation. The algorithm or method used by the validation system or MCS to generate the voucher validation number shall guarantee an insignificant percentage of repetitive validation numbers.
- (2) Gaming-device-generated validation number (system seed). The validation system shall send a unique seed to the gaming device upon enrolling the gaming device as voucher-printing-capable. The system subsequently may send a new seed to the gaming device after a voucher is printed. The algorithm or methods used to determine the seed shall guarantee an insignificant percentage of repetitive validation numbers.

(e) *Algorithm for generating offline voucher authentication identifiers*. If supported, the offline authentication identifier shall be of a unique value that is derived by a hash or other secure encryption method of at least 128 bits, that uniquely will identify the wager instrument, verify that the redeeming system was also the issuing system and validate the amount of the voucher. The following minimum set of input shall be used to create the authentication identifier:

- (1) slot machine identifier;
- (2) validation number;
- (3) voucher amount; and

(4) secure seed, key, etc. provided by the validation system or MCS to the gaming device.

(i) Secure seeds, keys, etc. as assigned shall be sufficiently random. Measures to avoid predictability will be reviewed by the licensed independent testing laboratory pursuant to Part 5318 of this Subchapter on a case-by-case basis.

(ii) The minimum length for any secure seeds, keys, etc. employed by the validation system or MCS shall be chosen from a pool of the variable type specified by the communication protocol used. The pool shall comprise at least 10 to the power of 14 randomly distributed values.

(f) *System voucher records.*

(1) The validation system shall retrieve the voucher information correctly based on the secure communication protocol implemented and store the voucher information into a database.

(2) The voucher record on the host system shall contain at a minimum the following voucher information:

(i) validation number;

(ii) date and time the gaming device printed the voucher (24-hour format that is understood by the local date and time format);

(iii) type of transaction or other method of differentiating voucher types (assuming multiple voucher types are available);

(iv) numeric value of voucher in dollars and cents;

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

(vi) date and time the voucher will expire (24-hour format that is understood by the local date and time format or expiration period from date of issuance), if applicable;

(vii) Machine number (or cashier or change booth location number, if voucher creation outside the gaming device is supported) that identifies the location from which the voucher was issued.

(g) *System requirements for offline ticketing support.* Offline ticketing shall:

(1) support the identification and redemption of offline vouchers through a system provided application;

(2) log all access and operations of users of the application described in paragraph (1) of this subdivision for 14 days through archived data or restoration from backup where maintaining such data on a live database is deemed inappropriate;

(3) the validation system or MCS shall set a maximum expiration length of no more than 30 gaming days for all provided and still-unused validation numbers and seed, key, etc. values;

(4) expired validation numbers and seed, key, etc. values shall be discarded in a way that prevents the re-use of unique combinations of validation numbers and seed, key, etc. values for a sufficient period of time on the system.

(h) *Voucher printing during loss of communication with validation system.* For validation systems that communicate to a gaming device through an interface board (also called a system machine interface board), if any links between the interface board and the MCS database go down, the interface board shall:

(1) not respond to the validation request from the gaming device and stop voucher printing;

(2) prevent the gaming device from further voucher issuance; and

(3) not read or store any further voucher information generated by the gaming device.

A maximum of two vouchers directly after loss of communication is acceptable, in cases where the interface element already has been seeded by the system, so long as the voucher issuance information is sent immediately, when communication is reestablished.

(i) *Online voucher redemption.* Vouchers can be redeemed at a gaming device, cashier or change booths or other approved validation terminals (kiosks), so long as such locations are enrolled for voucher validation with a validation system.

(1) The validation system shall process voucher redemption correctly according to the secure communication protocol implemented;

(2) The validation system shall update the voucher status on the database during each phase of the redemption process accordingly, so that whenever the voucher status changes, the system updates the database. Upon each status change, the database shall indicate the following information:

(i) date and time of status change;

(ii) voucher status;

(iii) voucher value;

(iv) machine number or source identification from where the voucher information came from.

(j) *Offline voucher redemption.* If supported, offline vouchers can be redeemed at a cashier or change booth, so long as such locations are enrolled for voucher validation with a validation system.

(1) The validation system at a minimum shall support the identification and redemption of offline vouchers through a system-provided application.

(2) The validation system shall process offline voucher redemption correctly according to the secure communication protocol implemented.

(3) The validation system shall update the voucher status on the database during each phase of the redemption process accordingly. In other words, whenever the voucher status changes, the system shall update the database. Upon each status change, the database shall indicate the following information:

(i) date and time of status change;

(ii) ticket/voucher status;

(iii) ticket/voucher value;

(iv) machine number or source identification from where the voucher information came.

(k) *Cashier and change booth operation.* All validation terminals shall be user-controlled and password-controlled. When a voucher is presented for redemption, a cashier:

(1) shall scan the bar code via an optical reader or equivalent; or

(2) shall input the voucher validation number manually; and

(3) may print a validation receipt, after the voucher is electronically validated, if applicable.

(l) *Validation receipt information.* Any validation receipt, at a minimum, shall contain the following printed information:

(1) machine number;

(2) validation number;

(3) date and time paid;

(4) amount; and

(5) cashier or change booth identifier.

(m) *Invalid voucher notification.* The validation system or MCS shall have the ability to identify the following occurrences and notify the cashier that one of the following conditions exists:

(1) voucher cannot be found on file (e.g., stale date, forgery, etc.);

(2) voucher has already been paid; or

(3) amount of voucher differs from amount on file. This requirement of this paragraph can be met by display of the voucher amount for confirmation by cashier during the redemption process).

(n) *Voucher redemption during communication loss.* If the online data system temporarily goes down and validation information cannot be sent to the validation system or MCS, an alternate method of payment shall be provided either by the validation system possessing unique features (e.g., validity checking of voucher information in conjunction with local database storage), to identify duplicate vouchers and prevent fraud by reprinting and redeeming a voucher that was previously issued by the gaming device; or use of an approved alternative method as designated by the commission that will accomplish the same. A maximum of two vouchers directly after loss of communication is acceptable, in cases where the interface element has already been seeded by the system, so long as the voucher issuance information is sent immediately, when communication is reestablished. This subdivision does not apply to systems employing an approved offline voucher routine.

(o) *Redemption terminals (kiosks).* Refer to Part 5316 for technical standards for redemption terminals.

(p) *Reporting requirements.* The following reports shall be generated at a minimum and reconciled with all validated/redeemed vouchers:

(1) voucher issuance report;

(2) voucher redemption report;

(3) voucher liability report;

(4) voucher drop variance report;

(5) transaction detail report, which shall be available from the validation system that shows all vouchers generated by a gaming device and all vouchers redeemed by the validation terminal or other gaming device; and

(6) cashier report, which shall detail individual vouchers, the sum of the vouchers paid by a cashier or change booth or redemption terminal.

The requirements set forth in paragraphs (2) and (4) of this subdivision shall not apply where two-part vouchers exist for the gaming device wherein the first part is dispensed as an original voucher to the patron and the second part remains attached to the printer mechanism as a copy (on a continuous roll) in such gaming device.

(q) *Database and validation component security.* Once validation information is stored in the database, such data shall not be altered in any way. The validation system database shall be encrypted or password-protected and shall possess a non-alterable user audit trail to prevent unauthorized access. The normal operation of any device that holds voucher information shall not have any options or method that may compromise voucher information. Any device that holds voucher information in its memory shall not allow removing of the information unless it has first transferred that information to the database or other secured component, or components, of the validation system.

§ 5317.40. System environmental and safety requirements.

(a) *Hardware and player safety.* Electrical and mechanical parts and design principles of the electronic associated hardware shall not subject a player to any physical hazards.

(b) *Environmental effects on system integrity standard.* A licensed independent testing laboratory shall perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. An online system shall be able to withstand the following tests, resuming game play without operator intervention:

(1) Electromagnetic interference. Systems shall not create electronic noise that affects the integrity or fairness of the neighboring associated equipment.

(2) Electrostatic interference. Protection against static discharges requires that the system's hardware be grounded in such a way that static discharge energy shall not damage or inhibit the normal operation of the electronics or other components within the system. A system may exhibit temporary disruption when subjected to a significant electrostatic discharge greater than human-body discharge, but such system shall exhibit a capacity to recover and complete any interrupted function without loss or corruption of any control or data information associated with such system. Such tests shall be conducted with a severity level of up to 27 kilovolts air discharge.