

***§543.33 What are the minimum internal control standards for surveillance for Tier B gaming operations?***

**Written Comment (March):** It is our understanding that there is the technology that would allow for remote or vpn access to the surveillance system. Therefore, we recommend introducing controls that would provide for the protection of the data on the servers that are a part of the surveillance system comparable to those found in the proposed IT section of the MICS.

**Response:** The Committee previously reviewed the surveillance section and did not make any recommendations that controls specific to the computerized systems utilized be considered. It is noteworthy that the MICS are intended to represent only the minimum controls necessary to assure the appropriate authorization, recognition and recordation of gaming and gaming related transactions and activities. The IT department has responsibility for systems involved in the collection of gaming related transactional data to facilitate its recognition and recordation. Not least of these functions is the collection of game performance data that revenue audit requires. If the gaming operation has server based games, not only do the IT systems collect operational data but they are also involved in the maintenance of game software directly involved in the determination of winning wagers.

Although the computer systems of the surveillance department are important to the effective operation of the facility, the systems do not rise to the level of those of the IT department and, as a result, the NIGC has determined that there is not sufficient justification to include mandatory controls in the MICS. The comment has no bearing on the transition from 542 to 543.

- (a) The surveillance system shall be maintained and operated from a surveillance operation room(s).
- (b) The entrance to the surveillance operation room shall be appropriately secured to prevent unauthorized access.
- (c) Access to the surveillance operation room shall be limited to surveillance personnel, designated staff, and other persons authorized in accordance with the surveillance department policy. The surveillance department shall maintain a sign-in log of other authorized persons entering the surveillance operation room.

(d) Surveillance operation room equipment shall have total override capability over all other satellite surveillance equipment located outside the surveillance operation room.

(e) The surveillance system shall include date and time generators that possess the capability to display the date and time of recorded events on video and/or digital recordings. The displayed date and time shall not significantly obstruct the recorded view.

(f) The surveillance operation room shall be attended at all times by personnel trained in the use of the equipment, knowledge of the games, and house rules. When necessary, surveillance operation rooms may be unattended for periods of time not to exceed 1 hour in any 8-hour period to allow appropriate meal and rest breaks.

(g) Each camera required by the standards in this section shall be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled by patrons or staff.

(h) Each camera required by the standards in this section shall possess the capability of having its picture displayed on a monitor and recorded. The surveillance system shall include sufficient numbers of monitors and recorders to simultaneously display and record multiple gaming and count room activities, and shall record the views of all dedicated cameras and motion activated dedicated cameras.

(i) Reasonable effort shall be made to repair each malfunction of surveillance system equipment required by the standards in this section within seventy-two (72) hours after the malfunction is discovered.

(1) In the event of a dedicated camera malfunction, the gaming operation and/or the surveillance department shall immediately provide alternative camera coverage or other

security measures, such as additional supervisory or security personnel, to protect the subject activity.

(2) The Tribal gaming regulatory authority shall be notified immediately of any required camera(s) that has malfunctioned for more than twenty-four (24) hours (or a shorter period as determined by the Tribal gaming regulatory authority), resulting in coverage or clarity that does not meet the requirements of this part.

(j) *Bingo.* (1) The surveillance system shall possess the capability to monitor the bingo ball drawing device or random number generator, which shall be recorded during the course of the draw by a dedicated camera with sufficient clarity to identify the balls drawn or numbers selected.

**Written Comment** (March): The issue that needs to be monitored is when human interaction is needed to read the ball draw. This surveillance standard is not possible to comply for linked electronic bingo systems and should be revised accordingly.

**Response:** The Committee reviewed the proposed standard and had no comment. It is self-evident from the standard that it does not apply to linked electronic bingo games but applies to a game that uses a ball draw, rabbit ears or blower or a board that reflects the numbers selected by an random number generator. This comment has no bearing on the transition from 542 to 543.

(2) The surveillance system shall monitor and record the game board and the activities of the personnel responsible for drawing, calling, and entering the balls drawn or numbers selected.

(k) *Card games.* The surveillance system shall monitor and record general activities in each card room with sufficient clarity to view patrons, dealers, and activities on the card table surfaces.

(1) *Player interfaces.* (1) Player interfaces offering a prize payout of \$250,000 or more shall be monitored and recorded by a dedicated camera(s) to provide coverage of:

(i) All patrons and staff at the player interface, and

(ii) The face of the player interface, with sufficient clarity to identify the prize payout line(s) of the player interface.

(iii) The coverage required in paragraphs (1)(1)(i) and (1)(1)(ii) does not require one dedicated camera per player interface if one dedicated camera is able to provide the required coverage for more than one player interface.

(2) The requirements in paragraph (1)(1) do not apply to wide area progressive player interfaces that are monitored by an independent vendor utilizing a linked on-line progressive computer system that have less than a 25% probability of a prize payout of \$3,000,000 or more.

(3) The requirements in paragraph (1) (1) do not apply to in-house progressive player interfaces that have less than a 25% probability of a prize payout of \$250,000 or more.

(4) Probability calculations for paragraphs (1) (2) and (1) (3) shall be performed using a formula provided by the Commission.

**Written Comment (March):** Put the formula in the regulation; it is our opinion that this formula needs to have the same formal comment period.

**Response:** The Committee reviewed the proposed standard and one comment was received that NIGC staff addressed. With regard to the formula being included in the regulation, it is anticipated that the complexity of paytables will evolve and the formula may need to be modified or additional calculations provided; Therefore, the ability to readily change the formula needs to be afforded. Furthermore, it is important to recognize that the MICS does not preclude a tribe from developing an alternative method of confirming the 25% probability that is equivalent to the NIGC formula, refer Part 542.3(c) (1). The comment has no bearing on the transition from 542 to 543.

(m) *Cage and vault.* (1) The surveillance system shall monitor and record a general overview of activities occurring in each cage and vault area with sufficient clarity to identify individuals within the cage and patrons and staff members at the counter areas and to confirm cash transactions occurring between staff members and between staff members and patrons.

**Note (May):** In the course of a discussion of another section, it became apparent that there was some confusion as to the meaning of the proposed addition to (q) (1). The standard has been revised to improve clarity.

*Revision incorporating May note:*

(1) The surveillance system shall monitor and record a general overview of activities occurring in each cage and vault area with sufficient clarity to identify individuals within the cage and patrons and staff members at the counter areas and to confirm **the amount of each** cash transactions occurring between staff members and between staff members and patrons.

(2) Each cashier station shall be equipped with one (1) dedicated overhead camera covering the transaction area.

(3) The cage or vault area in which fills and credits are transacted shall be monitored and recorded by a dedicated camera or motion activated dedicated camera that provides coverage with sufficient clarity to identify the chip values and the amounts on the fill and credit slips. Controls provided by a computerized fill and credit system may constitute an adequate alternative to viewing the amounts on the fill and credit slips.

(n) *Count rooms* (1) The surveillance system shall monitor and record with sufficient clarity all areas where coin may be stored or counted, including the hard\_count room, all

doors to the hard count room, all scales and wrapping machines, and all areas where uncounted coin may be stored during the drop and count process.

(2) The surveillance system shall provide coverage of scales of sufficient clarity to view any attempted manipulation of the recorded data.

(3) The surveillance system shall monitor and record with sufficient clarity all areas where currency may be stored or counted, and shall include the following:

(i) Soft count room including all doors to the room, all financial instrument storage components, safes, counting surfaces, and all count team personnel.

(ii) The counting surface area must be continuously monitored/displayed and recorded by a dedicated camera during the soft count.

(iii) The financial instrument storage component storage rack or area by either a dedicated camera or a motion- activated dedicated camera.

(iv) For count rooms utilizing currency counters and currency sorters, the surveillance system must possess the capability to monitor and record all areas where currency is sorted, stacked, counted, verified or stored during the count process. Coverage of the currency counting machines and currency sorting machines must be sufficiently clear to view the currency input, output and reject areas.

(o) *Video recording and/or digital record retention.* (1) All video recordings and/or digital records of coverage provided by dedicated cameras or motion-activated dedicated cameras required by the standards in this section shall be retained for a minimum of seven (7) days, or such longer period that may be required by the Tribal gaming regulatory authority.

(2) Recordings involving suspected or confirmed gaming crimes, unlawful activity, or detentions by security personnel, must be retained for a minimum of thirty (30) days, or such longer period that may be required by the Tribal gaming regulatory authority.

(3) Duly authenticated copies of video recordings and/or digital records shall be provided to the Commission upon request.

(p) *Video library log.* A video library log, or comparable alternative procedure, shall be maintained to demonstrate compliance with the storage, identification, and retention standards required in this section.

(q) *Malfunction and repair log.* (1) Surveillance personnel shall maintain a log or alternative procedure that documents each malfunction and repair of the surveillance system as defined in this section.

(2) The log shall state the time, date, and nature of each malfunction, the efforts expended to repair the malfunction and the date of each effort, the reasons for any delays in repairing the malfunction, the date the malfunction is repaired, and where applicable, any alternative security measures that were taken.

(3) The log must be retained for a minimum of 1 year after the date of the last entry in it.

(r) *Surveillance log.* (1) Surveillance personnel shall maintain a log of all surveillance activities.

(2) Such log shall be maintained by surveillance operation room personnel and shall be stored securely within the surveillance department.

(3) At a minimum, the following information shall be recorded in a surveillance log:

(i) Date;

(ii) Time commenced and terminated;

- (iii) Activity observed or performed; and
- (iv) The name or license credential number of each person who initiates, performs, or supervises the surveillance.
- (4) Surveillance personnel shall also record a summary of the results of the surveillance of any suspicious activity. This summary may be maintained in a separate log.
- (5) The log must be retained for a minimum of 1 year after the date of the last entry in it.
- (s) *Digital Surveillance System Standards* (1) The digital surveillance equipment used to satisfy the surveillance standards in this section shall:
  - (i) Record and play back video at a minimum of 30 frames per second (FPS), full screen (4 common intermediate format CIF), in real time.
  - (ii) Produce visual resolution that is adequate to satisfy the sufficient clarity standards in this section.
  - (iii) Have adequate storage capacity to maintain for a period of not less than seven (7) days, all images obtained from the video cameras.
  - (iv) Have a failure notification system that provides audible and visual notification of any failure in the surveillance system or the Digital Video Recording (DVR) media storage system. Alternatively, daily verification of the effective operation of surveillance system and DVR media storage system components is acceptable.
  - (v) Have a media storage system that is configured so that a failure of any single component will result in no loss of data from the media storage system.
- (2) Access, or the ability to access, a digital surveillance system from any location outside of the surveillance operation room, shall be approved by the Tribal gaming



regulatory authority. Such transmissions shall be effectively encrypted, firewalled on both ends, and password protected.

(3) All digital video disks or other storage media produced from the DVR system shall contain the data with the time and date it was recorded superimposed, the media player and the software necessary to view the DVR images, as well as a video verification encryption code (also known as a watermark).

(4) In the event of a failure of a DVR storage media system (total system failure), the gaming operation should strive to repair or replace the equipment within 8 hours of the failure.

(5) All DVR equipment must be located in a surveillance operation room(s) and the Surveillance Department shall be ultimately responsible for its proper operation and maintenance.

**Written Comment (March):** We recommend removing the words “surveillance operation room” and replacing them with “a secure area” in order to avoid any potential conflicts with the proposed definition for “SOR”. Also, as this standard currently reads, it may also prevent the sharing of resources with IT server locations as both are secure areas with the same level of security and climate control issues, fire suppression, etc.

**Response:** The Committee reviewed the proposed regulation and had no comment. The physical location of Surveillance equipment does not preclude such equipment from sharing floor space resources with the operation's Information Technology equipment. Due to space limitations, both Surveillance and IT hardware, as well as select operations, may inevitably share the same secured, climate-controlled physical environment. However, the surveillance equipment, operations and management, as well as IT equipment, and its operations and management, shall reside under each function's respective Departments. As such, “surveillance operation room” may correspondingly be considered an “IT operation room”. The comment has no bearing on the transition from 542 to 543.

**Note (May):** Following discussion during the conference call, it was decided to change “a surveillance operation room” to “a secured area”.

*Proposed revision as a result of May note:*

(5) All DVR equipment must be located in a ~~surveillance operation room(s)~~ **secured area** and the Surveillance Department shall be ultimately responsible for its proper operation and maintenance.