BULLETIN

Date: March 21, 2007

Subject: Advisory Bulletin on Digital Surveillance Systems

The objective of this Bulletin is to identify accepted gaming industry standards for a digital surveillance system. These guidelines are being offered for management and Tribal gaming regulatory authorities to consider, as they may deem appropriate, in the procurement, installation and oversight of a digital surveillance system. This Bulletin was developed in consultation with experts in the surveillance industry and Tribal gaming regulators and is intended to highlight practices that have gained broad acceptance throughout the gaming industry.

Due to the inherent vulnerabilities of a cash-intensive business, particularly one such as gaming in which asset-related transactions are occurring at a

rapid rate and often are not supported by an auditable document trail, the surveillance function is a key component of the organization's system of internal controls. Consequently, the NIGC recommends the following minimum technical specifications for a digital surveillance system.

Frame Rate

A recording rate of thirty (30) frames per second (FPS) is recommended for areas where gaming is conducted and where currency, coin and equivalents are counted, stored, accessed and transacted. A frame is the standard for measurement of video playback speed. It represents a single still picture in a sequence of pictures that gives the illusion of motion. Two interlacing fields of color, one vertical and the other horizontal constitute one frame. The recording rate of 30 FPS is considered real-time. Gaming activities and areas of currency, coin and equivalents include but are not limited to; table games, gaming machines, cage, vault, count room and other monetary transactions. A recording rate of fifteen (15) FPS is recommended for non-gaming public areas. A recording rate of 7.5 FPS is recommended for non-gaming limited public areas.

Resolution

A minimum 4 Common Intermediate Format (CIF) is recommended for live and recorded format systems. Essentially, the CIF rating refers to the vertical and horizontal lines of color on a TV screen. The higher the CIF rating is; the more crisp the picture. CIF is a standard video format used for videoconferences and is ¼ the size of a TV display. 4CIF is large enough to match the video size and quality of a TV display and is considered full resolution.

Compression

A video record that is being transferred to and stored on a computer hard drive or other storage medium will consume huge amounts of memory; therefore, the data is normally compressed to reduce the storage area requirement. Technically, compression is the translation of a digital image data into a format which requires less storage than the original data. The digital surveillance system should be able to compress and decompress (restore) stored video data to 4CIF.

Retention

A fourteen (14) day retention period is recommended for table game drops, gaming machine drops, count room activity, main bank, cage cashier and other monetary transactions, when feasible, to substantiate cash and cash equivalent transactions for audit purposes. At a minimum, a seven (7) day retention period is recommended for other video data.

Fail Over

It is recommended that the digital surveillance system be configured so that no single component failure immobilizes the entire system. To ensure the digital system remains operational, any component failure should result in an audio and visual notification.

Data retention should be configured to prevent loss of data. Redundant equipment configured to automatically switch over if primary equipment fails is recommended. It is also recommended that spare equipment be maintained on site to ensure a reasonable level of protection in the event of primary equipment failure.

Network Structure

It is prudent for the digital surveillance system network to be separate from the main operating network of the gaming enterprise. Likewise, system wiring should be secured to prevent unauthorized access or tampering. If the system is to be integrated into an existing network, it is highly recommended that system traffic be safeguarded to prevent unauthorized access to data.

Accepted practice would dictate that access to the network be well documented for audit purposes. Documentation should consist of a written or electronic record containing identifying information about the individual, the time, the date, the duration and the purpose for the access.

Video Files

It is highly recommended that each video file maintained for evidentiary purposes include the date and time it was recorded and the name of the individual who recorded it. Procedures should also be developed to physically safeguard the integrity of video data maintained for evidentiary purposes in a secure area.

Furthermore, it is suggested that storage media for evidentiary purposes include an associated media player on which the video file can be viewed. The video file should include a verification code (watermark) to prove authenticity.

Component Failures

We would advise that the each system possess sufficient redundancy and spare parts to ensure the surveillance department remains operational or at least can quickly recover vital functions in the event of a component failure. It is recommended that the repair or replacement of equipment

causing a component failure be performed within four (4) hours of the audio and visual notification. Component failures should also be documented on a written or electronic surveillance malfunction log. Camera equipment repair or replacement is typically required to be handled within 72 hours of failure.

Responsibility for the System

Ensuring the continued operation and effective maintenance of the system necessitates ongoing training of the surveillance technicians and specific problems may occasionally warrant assistance from the manufacturer.

Cooling and Electrical Considerations

A digital surveillance system can generate a massive amount of heat and consume a large amount of electricity; therefore, careful attention to the sufficiency of the cooling system is suggested to prevent component failures. Additionally, installation of an uninterrupted power source (UPS) is recommended to ensure proper operation in the event of a power interruption.

Documentation of Unusual Occurrences

Best practices would stipulate that a written record documenting any unusual occurrence needs to be prepared and forwarded to appropriate supervisory personnel. Unusual occurrences include, but are not limited to, a system failure, which was not repaired or replaced, granting of remote access to the system and an upgrade or change to any part of the system configuration.