BULLETIN

No. 2008

March 21, 2007

Subject: Server Based Gaming Network Review and Security Measures Advisory

To: Region V Tribal Gaming Commissions

From: Tim Harper, Region Director

Subject: Server-Based Gaming Network Review and Security Measures Advisory

Server-based gaming is widely used in Tribal gaming operations throughout NIGC Region V, which includes Oklahoma, Texas, and Kansas. As a result, this office **highly recommends** that Tribes, Tribal Gaming Regulatory Agencies, and gaming operations take precautionary measures to ensure the integrity and security of these games to protect the Tribes' gaming revenue.

Server-based gaming differs from stand-alone type gaming, and, therefore, has its own inherent weaknesses and vulnerabilities that should be addressed. In an effort to assist Tribes in securing such gaming systems, the National Indian Gaming Commission retained an independent computer technologies group to undertake a special review and analysis related to gaming software systems being utilized by a number of gaming tribes specifically in Oklahoma. The objective of this examination was to determine the level of security related to the physical and network access to such systems. The review included:

· Network configuration;

· Gaming operation access controls for vendors to gaming equipment and computer servers;

· Any security measures employed by the gaming operation; and

· Casino compliance reporting methods and procedures for server based gaming vendors.

The following summarizes the security vulnerabilities identified:

- **Open and uncontrolled network connections**. Due to the network configuration of many systems, the gaming operation is not able to monitor the activity of any particular vendor. A vendor may have independent and uncontrolled network connections directly to the gaming machines. Given this type of system setup a vendor could make modifications to the system without the gaming operation's knowledge or approval.

- **Lack of Sufficient Auditing Mechanisms**. Many gaming operations do not have the ability to review, audit and approve reports provided by a vendor. Many current network configurations potentially allow a vendor to change and otherwise manipulate the data in each server without the knowledge or consent of the gaming operations. Some gaming operations do not have the ability to access the server data at all.

- **Network Availability**. It is our observation that many gaming networks are not adequately secured from unauthorized access. Many systems have several points of connectivity which may not be monitored and could potentially cause a network disruption. Procedures ought to be implemented to secure the network against unauthorized access that may result in system failures and lost data.

- **Lack of Security Incident Response Plans and Procedures**. In many gaming operations there is no security policy or contingency plan in place to respond to unauthorized access, incident detection, and data or system recovery. Such a plan should provide a security response to secure the network and damage containment.

- **Lack of Secure Upgrade Mechanisms and Procedures**. Our review of common network procedures did not identify procedures for completion of upgrades for security and software. The procedures failed to identify an administrator and control such upgrades.

As a result of this review, we are providing the following guidance which in certain instances underscores the importance of complying with specific provisions Indian Gaming Regulatory Act (IGRA), 25 U.S.C. § 2701 *et seq.* and NIGC regulations, 25 C.F.R. Parts 501-599, and in other instances includes suggestions for implementing measures to aid Tribes in protecting their gaming operations:

+ Implement policies and procedures to secure access to servers and communication equipment for server-based games. *See* 25 C.F.R. § 542.16; *see also*25 C.F.R. §§ 542.7 and 542.13. Specifically, servers and communication equipment should be housed in secure, dedicated rooms or cabinets to provide physical security measures. Access to these areas should be controlled and documented. At minimum, such documentation should include the date and time of access, printed name, and signature. Further, surveillance cameras should be utilized to provide coverage of these sensitive areas and video should be monitored, recorded, and retained for an adequate period of time. Regulations require that recorded video be retained a minimum of seven (7) days. However, retaining recorded video for thirty (30) days may be more appropriate to allow for issues and incidents to be reported and reviewed.

+ Ensure that employees who are custodians of gaming devices, including employees that have access to cash and accounting records within such devices, are subject to background investigations and licensing requirements. *See* 25 C.F.R. § 502.14(a)(10); 25 U.S.C. § 2710(b)(2)(F). These employees include those who perform duties relating to server-based gaming systems, such as gaming machine techs, IT staff, gaming machine floor supervisors, and jackpot payout clerks. Ultimately, background investigation and licensing procedures provide a vetting process for employees being

placed into these very important key positions.;

+ License gaming machine vendors and technicians, as required by several Tribal gaming ordinances and State Compacts, to ensure that persons associated with these companies are properly vetted before being allowed into your Tribal gaming operation.;

+ Devise a security, contingency, continuity, disaster, or incident response plan that addresses Information Technology and server-based gaming operations.;

+ Implement an Intrusion Detection System (IDS) for the IT system to provide notification in the event of an attack, loss of network availability, or unauthorized access to the system.

+ Utilize servers with operating systems that have discretionary access controls and firewalls which are in place and operational. Further, a Virtual Private Network (VPN) Concentrator can provide a security layer against unauthorized access to the server when properly configured and maintained.;

+ Require gaming machine vendors to provide a current list of their employees assigned to service each Tribe's gaming operations. The gaming machine vendor employees should provide proper identification prior to being allowed access to gaming machines on the casino floor, casino back of house areas, and secured areas where gaming machine servers are located. A network vulnerability and penetration assessment test should be performed periodically to determine the effectiveness of the procedures and protections that are in place.

If you have any questions concerning this or other matters, please do not hesitate to contact the NIGC Regional Office in Tulsa at (918) 581-7924. Thank you for your attention to this very important matter.