GAMING INDUSTRY BULLETIN 46

December 10, 2002
Revised February 27, 2012

WIRELESS LOCAL AREA NETWORKS (WLANs)

The Colorado Division of Gaming has learned some licensees are interested in utilizing 802.11(x) WLAN technology for casino gaming operations. Implementing 802.11n is relatively inexpensive and provides a transparent and easy wireless connection while offering strong performance. Unfortunately, this convenience can increase the risk of a security breach. Organizations with deployed WLANs are more vulnerable to unauthorized use of, and access to, their internal infrastructure.

At this time, the Division does not recognize WLANs as an approved technology due to security concerns. Under no circumstances are casinos authorized to utilize WLANs for any activity that can, or has the potential to, impact gaming transactions, game accounting data, slot monitoring systems transactions and/or data, or the calculation and/or reporting of adjusted gross proceeds (AGP).

The main security protocol for WLANs is Wi-fi Protected Access (WEP, WPA/WPA2). WEP, WPA/WPA2 is a user authentification and data encryption system which was designed to provide confidentiality for network traffic using the wireless protocol. However, security concerns persist because:

1. The radio transmissions travel through the air and can be intercepted
2. Vulnerabilities in WEP, WPA/WPA2 enable a talented hacker to break into the wireless network. Using a custom made antenna, a hacker can collect enough wireless packets from a remote safe distance to determine how to break into a wireless network.

Until subsequent WLAN standards adequately address the security concerns, the Division feels that wireless-enabled networks are not secure and are inappropriate for casino gaming operations. If you have any questions, please contact any member of the Technical Systems Group.