Surveillance – Audit
25 CFR 543.21 Toolkit

Version 1.0

Division of Public Affairs

NIGC Surveillance Toolkit–25 CFR 543.21

Over thirty years ago, Congress adopted the Indian Gaming Regulatory Act (IGRA) to provide a statutory basis for gaming by Indian tribes. IGRA establishes the National Indian Gaming Commission (NIGC) to regulate and provide oversight for gaming activities conducted by sovereign Indian tribes on Indian lands. The mission of the NIGC is to realize IGRA's goals: (1) promoting tribal economic development, self-sufficiency and strong tribal governments; (2) maintaining the integrity of the Indian gaming industry; and (3) ensuring that tribes are the primary beneficiaries of their gaming activities. As a primary means to accomplish these goals, NIGC provides training and technical assistance to Indian tribes, specifically for Gaming Operations and Regulators.

The NIGC is pleased to present this Toolkit to all stakeholders of Indian Gaming. This reference guide assists Auditors, Regulators, and Operations personnel in the performance of measuring compliance of their operation(s) with 25 CFR 543.21 and additional 25 CFR 543 standards relevant to Surveillance Operations. The Toolkit design provides each 543.21 standard, intent of each standard, and a recommended testing step to ensure minimum regulatory compliance.

Additionally, this Toolkit design meets the minimum requirements of the NIGC Minimum Internal Control Standards (MICS). The Tribal Internal Control Standards (TICS) and/or System of Internal Control Standards (SICS) may require further testing which is not included in this Toolkit. The uniqueness of each gaming operation warrants a robust set of controls tailored to its individual needs.

If you have questions or comments about this guide, please contact the NIGC Division of Public Affairs at traininginfo@nigc.gov. For more information, visit the NIGC website at https://www.nigc.gov.

How to use this Toolkit

The Training Department has designed this toolkit as a resource for understanding the Surveillance 543.21 Minimum Internal Control Standards (MICS) and as a tool for conducting an audit of the Surveillance department in determining compliance with 543.21.

This Toolkit table can help:

1. Clarify the meaning of terms used in this Toolkit (Definitions)
2. Learn the regulation for Surveillance 543.21. (The regulation is listed in the second column of the table verbatim)
3. Understand the intent of the regulation and importance of the control. (The intent is listed in the third column in the table)
4. Determine testing steps to determine compliance with the regulation. (The testing step is listed in the third column of the table under the intent information)
5. Identify best practices. (These have been included for some regulations in either the intent or testing steps to provide the user with current industry procedures) and
6. Consider practical advice when performing testing step. (Example: step completed in another section. Additional information is provided as a Note)

The Toolkit provides many practical and concrete suggestions for understanding and evaluating 543.21compliance. Either the new or the experienced auditor will find this Toolkit helpful during various stages of the audit.

GLOSSARY	DEFINITION
Agent	A person authorized by the gaming operation, as approved by the TGRA, to make decisions or perform assigned tasks or actions on behalf of the gaming operation.
Cage	A secure work area within the gaming operation for cashiers, which may include a storage area for the gaming operation bankroll.
Cash equivalents	Documents, financial instruments other than cash, or anything else of representative value to which the gaming operation has assigned a monetary value. A cash equivalent includes, but is not limited to, tokens, chips, coupons, vouchers, payout slips and tickets, and other items to which a gaming operation has assigned an exchange value.
Class II gaming	Class II gaming has the same meaning as defined in 25 U.S.C. 2703(7)(A).
Class II gaming system	All components, whether or not technologic aids in electronic, computer, mechanical, or other technologic form, that function together to aid the play of one or more Class II games, including accounting functions mandated by these regulations or part 547 of this chapter.
Count	The act of counting and recording the drop and/or other funds. In addition, the total funds counted for a particular game, player interface, shift, or other period.

GLOSSARY	DEFINITION
Count room	A secured room where the count is performed in which the cash and cash equivalents are counted.
Dedicated camera	A video camera that continuously records a specific activity.
Kiosk	A device capable of redeeming vouchers and/or wagering credits or initiating electronic transfers of money to or from a patron deposit account.
MICS	Minimum internal control standards.
Patron	A person who is a customer or guest of the gaming operation and may interact with a Class II game. Also, may be referred to as a “player".
Promotional progressive pots and/or pools	Funds contributed to a game by and for the benefit of players that are distributed to players based on a predetermined event.
Sufficient clarity	The capacity of a surveillance system to record images at a minimum of 20 frames per second or equivalent recording speed and at a resolution sufficient to clearly identify the intended activity, person, object, or location.
Surveillance operation room(s)	The secured area(s) where surveillance takes place and/or where active surveillance equipment is located.
Surveillance system	A system of video cameras, monitors, recorders, video printers, switches, selectors, and other equipment used for surveillance.

GLOSSARY	DEFINITION
SICS (System of Internal Control Standards)	An overall operational framework for a gaming operation that incorporates principles of independence and segregation of function, and is comprised of written policies, procedures, and standard practices based on overarching regulatory standards specifically designed to create a system of checks and balances to safeguard the integrity of a gaming operation and protect its assets from unauthorized access, misappropriation, forgery, theft, or fraud.
Tier A	Gaming operations with annual gross gaming revenues of more than $3 million but not more than $8 million.
Tier B	Gaming operations with annual gross gaming revenues of more than $8 million but not more than $15 million.
Tier C	Gaming operations with annual gross gaming revenues of more than $15 million.
TGRA	Tribal Gaming Regulatory Authority, which is the entity authorized by tribal law to regulate gaming conducted pursuant to the Indian Gaming Regulatory Act.
TICS	Tribal Internal Control Standards established by the TGRA that are at least as stringent as the standards set forth in the MICS.
Vault	A secure area where cash and cash equivalents are stored.
Voucher	A financial instrument of fixed wagering value, usually paper, that can be used only to acquire an equivalent value of cashable credits or cash through interaction with a voucher system.

Surveillance Minimum Internal Control Standards
§ 543.21

Citation	Language	Intent and Testing
543.21(a)	(a) *Supervision.* Supervision must be provided as needed for surveillance by an agent(s) with authority equal to or greater than those being supervised.	**Intent:** To provide for the proper supervision of surveillance staff by someone with authority equal to or greater than those being supervised. **Testing:** 1. Review Surveillance organizational chart, department schedules and/or job descriptions to determine supervisory responsibility and availability. 2. Review TICS and or SICS to determine supervisory procedures implemented (*e.g.,* designation of supervisory and non-supervisory agents, reporting responsibilities, etc.). 3. Identify and document titles of supervisory personnel. 4. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine who has supervision responsibility for the Surveillance Department. 5. Observe shift(s) to ensure that supervision requirements are being met. **Best Practices:** 1. Effective supervision should be by someone of greater authority than those being supervised. If supervision is of equal authority, consider additional controls that clearly distinguish the line of authority.
543.21(b)(1)	(b) *Surveillance equipment and control room(s).* Controls must be established and procedures implemented that include the following: (1) For Tier A, the surveillance system must be maintained and operated from a secured location, such as a locked cabinet. For Tiers B and C, the surveillance system must be maintained	**Intent:** To prevent tampering with surveillance equipment and/or recordings, and to ensure no unauthorized access. Additionally, it is to actively deter, detect, and/or document potential threats to tribal assets and the integrity of gaming. This is accomplished by identifying individuals and activity, confirming the amounts of transactions, and documenting compliance with applicable internal control standards.

Citation	Language	Intent and Testing
	and operated from a staffed surveillance operation room(s).	**Note:** Tier A (as defined in Glossary) surveillance systems are not required to be staffed. **Testing:** 1. Review the gaming operation's annual gross gaming revenue to determine which Tier requirements apply (See Definitions for Tier thresholds). 2. Review TICS and/or SICS to determine whether controls for gaming operation surveillance equipment and control room(s) which meet the requirements for the appropriate Tier are established and implemented. 3. For Tier A gaming operations, (1) observe the surveillance equipment and note its surroundings (*e.g.,* within a locked room, a cabinet, etc.), (2) interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent, Security Officer) to identify security features, and (3) determine whether the surveillance system is operated from a secured location. 4. For Tier B or C, observe the surveillance room(s) for assigned staff. If no staff are present at the time of observation, inquire with appropriate surveillance personnel and department management to determine how the room is being staffed. 5. Review Surveillance department schedules to ensure appropriate staffing levels are maintained for Tier B and C operations. **Best Practices:** 1. For Tier A operations— a. Appropriate personnel (Surveillance Employees, Security Officers, or TGRA staff) should check the system at least once per day to verify the system is functioning properly and ensure the date and time are accurate. b. Use a surveillance system access log to document system checks, camera and recording device checks, and general system access.

Citation	Language	Intent and Testing
		c. Install a dedicated camera to continuously record the physical access point of the surveillance system. d. Use hardened doors and tamper resistant locks on cabinets and closets housing surveillance equipment. 2. For Tier B or C operations— a. Ensure adequate personnel are present in the room to monitor drop and count activities as well as other gaming activities occurring at the same time (Size and scope of the operation may dictate that one person is enough to monitor some shifts, but two or more persons may be needed during count and drop activities). b. Allow limited personal breaks during times when only one surveillance staff member is on duty but require those breaks to be in areas separate from other casino personnel so that it is not known the surveillance room is unoccupied. Ensure that surveillance agents are able to answer radio or phone transmissions from the break area(s). Generally, it is best to not reveal surveillance staffing levels to casino personnel.
543.21(b)(2)	(2) The surveillance operation room(s) must be secured to prevent unauthorized entry.	**Intent:** To ensure the surveillance operation room(s) are secured to prevent unauthorized persons from entering and or accessing sensitive equipment. **Testing:** 1. Review TICS and/or SICS to determine whether controls are established and implemented for surveillance operation room(s) being secured to prevent unauthorized entry . (**Note:** The regulations define surveillance operation room(s) as "The secured area(s) where surveillance takes place and/or where active surveillance equipment is located." This control therefore includes surveillance server rooms, IDF closets, electrical rooms and closets, and communication rooms and closets in the facility—anywhere active surveillance equipment is located.)

Citation	Language	Intent and Testing
		2. Note the location of the surveillance operation room(s) and accessibility from public or private areas of the gaming operation. 3. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine the location of all active surveillance equipment and how each area is secured. 4. Physically attempt to open the surveillance operation door(s) before disabling any locks. **Best Practices:** 1. Locate the surveillance operation room so that the entrance is not readily accessible or viewable. 2. In addition to securing the equipment against unauthorized entry, surveillance operations should consider requiring measures at installation to prevent surveillance equipment (*e.g.*, monitors, recording devices, selectors, switches, servers, cabling, patch panels, etc.) from being obstructed, tampered with or disabled.
543.21(b)(3)	(3) Access to the surveillance operation room(s) must be limited to surveillance agents and other authorized persons.	**Intent:** To ensure access to the surveillance operation room(s) is limited to surveillance agents and other authorized persons to prevent unauthorized personnel from entering. **Testing:** 1. Review TICS and/or SICS to determine whether controls to limit surveillance room access to surveillance agents and other authorized persons are established and implemented. (**Note:** The regulations define surveillance operation room(s) as "The secured area(s) where surveillance takes place and/or where active surveillance equipment is located." This control therefore includes surveillance server rooms, IDF closets, electrical rooms and closets, and communication rooms and closets in the facility—anywhere surveillance equipment is located.)

Citation	Language	Intent and Testing
		2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine who (*e.g.,* General Manager, TGRA staff, Security staff, gaming management, law enforcement, tribal officials) is authorized to enter the surveillance room, and the conditions upon which they may enter. 3. Review TICS and or SICS to determine whether there is an authorized access list. 4. Verify the Authorized Access List has been approved by either TGRA or Operations 5. Review surveillance access logs and compare them to the authorized access list. 6. If Surveillance Room key(s) are located within a computerized key tracking system, review who has authority to remove Surveillance Access Keys and compare to the approved access list. 7. Ask appropriate personnel who has keys/access to the surveillance room (*e.g.*, emergency keys, etc.). **Best Practices:** 1. Set up a separate room where appropriate Department Managers may review surveillance video without giving them access to the entire surveillance room. 2. Together with TGRA, establish a list of personnel who can access the room or surveillance system under specific conditions (*e.g.,* building maintenance, IT, janitorial, etc.). It is also recommended that the authorized access list be posted where agents can quickly reference.
543.21(b)(4)	(4) Surveillance operation room(s) access logs must be maintained.	**Intent:** To ensure that access to the surveillance equipment and control room(s) is restricted to authorized persons and that a list of all non-surveillance personnel entering the surveillance operation room(s).

Citation	Language	Intent and Testing
		Testing: 1. Review TICS and/or SICS to determine whether controls which require surveillance operation room(s) access logs to be maintained are established and implemented. (**Note:** The regulations define surveillance operation room(s) as "The secured area(s) where surveillance takes place and/or where active surveillance equipment is located." This control therefore includes surveillance server rooms, IDF closets, electrical rooms and closets, and communication rooms and closets in the facility—anywhere surveillance equipment is located.) 2. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine whether access logs are maintained and stored as required. 3. Review access logs to confirm that logs are maintained as required, that all required information is entered into the log, and that logs are current. Verify that the logs are being retained for at least five years (see part 571.7(c)). **Best Practice:** 1. The access log should include the date and time of entry and exit, reason for access, name (printed), position/title, and the agent authorizing access.
543.21(b)(5)	(5) Surveillance operation room equipment must have total override capability over all other satellite surveillance equipment.	**Intent:** To ensure that surveillance agents maintain complete and continuous access and control over all surveillance equipment. **Testing:** 1. Review TICS and/or SICS to determine whether controls which require the surveillance operation room equipment have total override capability over all other satellite surveillance equipment are established and implemented. 2. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance

Citation	Language	Intent and Testing
		Agent) to determine whether satellite viewing stations exist and if the surveillance room has override capability. Determine total number of viewing stations in operation throughout the gaming operation. Determine whether any person has access to the surveillance system through server access or other means. 3. Observe override capability of satellite surveillance equipment by the surveillance operation room. **Best Practice:** 1. Consider establishing a MOU with non-surveillance departments, which have viewing access to non-sensitive or sensitive cameras. Similar to a code of standards for surveillance staff, identify the use and conduct of surveillance cameras are for official use and monitored by the Surveillance staff, i.e., observations for personal use are prohibited. Have training provided for override capabilities and that the surveillance operations has priority and secondary viewer will relinquish control. 2. Recommend inquiry whether there is use of any other surveillance cameras or systems, such as remote viewing, which are not part of casino surveillance system. **Note:** 1. Some operations choose to allow non-surveillance departments (i.e., TGRA, security, table games management, or gaming management) access to specific cameras or recording devices. This control was created to ensure that Surveillance agent(s) could take control of all cameras and recording devices as needed.
543.21(b)(6) (i)-(ii)	(6) Power loss to the surveillance system: (i) For Tier A, in the event of power loss to the surveillance system, alternative security procedures, such as additional supervisory or	**Intent:** To ensure that procedures are in place in the event a power outage or catastrophic failure of the surveillance system occurs to reduce potential risk to assets.

Citation	Language	Intent and Testing
	security agents, must be implemented immediately. (ii) For Tier B and C, in the event of power loss to the surveillance system, an auxiliary or backup power source must be available and capable of providing immediate restoration of power to the surveillance system to ensure that surveillance agents can observe all areas covered by dedicated cameras.	**Testing:** 1. Review TICS and/or SICS to determine whether controls for the immediate implementation of alternative security procedures or an auxiliary or backup power source (depending on the Tier level of the gaming operation), in the event of a power loss to the surveillance system are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Security Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine the procedure for power outage(s) or other catastrophic failure of the surveillance system. For Tier B and C operations, interview appropriate personnel (e.g. Surveillance Manager/Director, Surveillance Shift Manager, Facility Manager, etc.) to determine whether the operation has an auxiliary or backup power source capable of immediate restoration of power to the surveillance system. 3. For Tier B and C gaming operations, review auxiliary or backup power source procedures to verify they provide for an immediate restoration of power to the surveillance system so that surveillance agents can observe all areas of the gaming operation covered by dedicated cameras. 4. TICS and/or SICS should also require periodic testing of the backup power source to ensure that it is "available and capable" to provide immediate restoration of power. Testing for this control should include reviewing backup generator weekly exercise logs and transfer switch periodic testing logs. **Note:** 1. A "backup power source" is typically a backup power generator or individual Uninterruptable Power Supply or Source (UPS). An "auxiliary power source" is typically an alternative power supplier, such as another electricity utility provider, a natural gas utility provider, or even alternative power supplies such as solar, wind, biofuels, or similar.

Citation	Language	Intent and Testing
		Best Practices: 1. If UPS units are utilized solely (without a backup power generator) to provide backup power to the surveillance equipment, testing should be performed to determine how long the surveillance system can safely operate before requiring to be powered down properly without damaging the surveillance system components. 2. Because UPS units provide limited functionality during a power loss to the surveillance system, operations should implement alternative security procedures along with the use of UPS units. 3. For Tier A gaming operations, verify that the alternative security procedures provide immediate additional security measures for areas deemed most vulnerable to theft. (*e.g.*, requirements for security and/or supervisory personnel to report to cash handling areas such as the Cage and Count Room (if count is active) and table games pits.) 4. Operations should have procedures for events where the power goes out to more than just the surveillance system. These procedures should include evacuation of the facility and securing of assets such as banks, tills, floats, etc. Controls should include additional areas that are deemed cash sensitive areas. 5. Surveillance management should request copies of these logs from Facilities Maintenance personnel for documentation purposes. Surveillance agents may also log system testing in daily activity reports. 6. Although emergency lighting systems are not necessarily included in the language of this control, Surveillance Management should test this system along with the backup power source and document results.

Citation	Language	Intent and Testing
543.21(b)(7)	(7) The surveillance system must record an accurate date and time stamp on recorded events. The displayed date and time must not significantly obstruct the recorded view.	**Intent:** To ensure that video footage is usable and reliable evidence in legal proceedings and other formal inquiries (*e.g.*, criminal prosecutions, insurance claims, human resources cases, and compliance documentation). The date and time stamp is also useful in searching for a particular date or time in reviewing footage. **Testing:** 1. Review TICS and/or SICS to determine whether controls for the surveillance system to record an accurate date/time stamp on recorded events. 2. Verify the date/time stamp does not significantly obstruct the recorded view are established and implemented. 3. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine the procedure for establishing what date and time source is used for the surveillance system settings. **Best Practices:** 1. Synchronize all gaming operation devices and systems that utilize a date/time stamp to one uniform source. 2. A common date and time source (e.g., atomic clock, phone system date/time, etc.) should be used for setting the time on the surveillance system. 3. Surveillance agent(s) should review the date/time stamp as part of the periodic camera checks, and document the results.
543.21(b)(8)	(8) All surveillance agents must be trained in the use of the equipment, games, and house rules.	**Intent:** To ensure that the agents are familiar with all surveillance equipment, its purpose and use. The activities they are observing and able to identify non-compliance with established controls and deviations from normal procedures.

Citation	Language	Intent and Testing
		Testing: 1. Review TICS and/or SICS to determine whether controls for all surveillance agents to receive training in the use of equipment, games, and house rules are established and implemented. 2. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine what training is provided, who receives it, how often training is provided, and the types of training programs in place. 3. Review training logs and training documentation in Surveillance personnel files to verify what training has been provided, who received it, how often training is provided, and the types of training programs in place. 4. Confirm that training programs and the training received includes "use of equipment, games, and house rules." **Best Practices:** 1. TGRA's and gaming operations should establish a minimum level of training for all surveillance agents in the TICS/SICS that is sufficient to equip employees with a complete understanding of the activities they are required to observe. 2. Agents should also receive training in common cheating techniques, effective surveillance techniques and methods, typical fraud/theft/scam schemes, and a familiarity with the MICS, TICS, and SICS.
543.21(b)(9)	(9) Each camera required by the standards in this section must be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled.	**Intent:** To protect the camera views being observed and recorded and the integrity of the surveillance system in general. Cameras, cabling, connections are installed out of reach and in such a manner as the view cannot be disabled, altered or obstructed.

Citation	Language	Intent and Testing
		Testing: 1. Review TICS and/or SICS to determine whether controls which ensure cameras are installed in a manner that prevents them from being readily obstructed, tampered with, or disabled are established and implemented. 2. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Technician) to determine what types of cameras are installed and how cameras and surveillance equipment are installed in order to prevent them from being readily obstructed, tampered with, or disabled. 3. Observe the gaming operation, paying particular attention to areas with low ceilings where cameras could be within reach. Observe the types of cameras installed in each area and note cameras that may be susceptible to being obstructed, tampered with, or disabled. (Best practices include installing cameras with tamper-resistant domes or so that they are out of reach and the direction that the camera is facing or moving is unknown.) **Best Practices:** 1. SICS should be developed in other departments (e.g., Bingo, Card Games, Gaming Promotions) that require Surveillance management to be notified of and approve changes to the gaming operation floor or installation of promotional signs and items placed on the gaming floor. This ensures that those changes and installations do not interfere or significantly obstruct required camera coverage. 2. Surveillance agents should also conduct periodic inspections (at least once per shift) of the surveillance system to identify any cameras that may have been obstructed, tampered with, or disabled.

Citation	Language	Intent and Testing
543.21(B)(10)(i)-(iv)	(10) The surveillance system must: (i) Have the capability to display all camera views on a monitor; (ii) Include sufficient numbers of recording devices to record the views of all cameras required by this section; (iii) Record all camera views (iv) For Tier B and C only, include sufficient numbers of monitors to simultaneously display gaming and count room activities.	**Intent:** The intent of this control is to ensure that Surveillance Agents have the technical capabilities (sufficient monitors and recording) to observe all activities (such as drops, payouts, transfers, accessing bill acceptors, and count room activities) that may occur simultaneously. **Testing:** 1. Review TICS and/or SICS to determine whether controls ensure the surveillance system has the capability to display all camera views on a monitor; includes a sufficient number of recording devices to record all camera views; records all camera views; and for Tier B and C gaming operations, includes sufficient numbers of monitors to display gaming and count room activities simultaneously are established and implemented. 2. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine whether (1) the surveillance system has the capability to display all camera views on a monitor, (2) includes a sufficient number of recording devices to record all camera views, (3) records all camera views, and for Tier B and C gaming operations, and (4) includes sufficient numbers of monitors to display gaming and count room activities simultaneously. 3. Observe the location of installed cameras on the gaming floor and make note of any camera views that do not appear to be displayed on surveillance monitors. Review recordings to determine whether any camera views are not being recorded as required. For Tier B and C only, observe the surveillance system to verify that there are sufficient numbers of monitors to display both gaming and count room activities simultaneously. **Notes:** 1. Cameras installed in the surveillance operation room itself that are designed solely to monitor surveillance room activities are not considered to be non-compliant with this control as they are recorded and can be displayed by Surveillance Management.

Citation	Language	Intent and Testing
		2. The requirement that the surveillance system include "sufficient numbers of recording devices to record the views of all cameras" is important as it may affect the ability of the system to remain compliant with the storage, identification, and retention standards referenced in 543.21(f)(1). If insufficient recording devices are available, some camera views may not be recorded (stored) as they normally would be. Some camera views may not be recorded at the required "sufficient clarity" (identification) setting of a minimum of 20 frames/images per second, as the recording system may automatically step down the recording frame rate to adjust to the reduced amount of storage media available. Also, if insufficient recording devices are available, the recorded video may not be retained for the minimum 7 days required due to the reduced amount of storage media. **Best Practices:** 1. "Dummy cameras" or fake cameras in order to give the appearance of increased camera coverage are not recommended, as these "cameras" cannot be recorded or displayed as required. Additionally, the use of these types of "cameras" may actually put the tribe at increased liability risk due to patrons or employees being given the impression that video surveillance of an incident is available when it is not. 2. One way to test whether there is a sufficient number of recording devices for all camera views would be to note the number of total cameras and the total number of recording devices/servers, then note how many cameras are assigned per recording device. 3. Refer to the SICS/TICS for the required retention requirements and then sample a number of cameras to see if the cameras are being retained for the required length. All digital storage devices should be checked routinely to ensure the standards are met, and more frequently when changes are made to the storage devices.

Citation	Language	Intent and Testing
543.21(b)(11)(i)–(ii)	(11) A periodic inspection of the surveillance systems must be conducted. When a malfunction of the surveillance system is discovered, the malfunction and necessary repairs must be documented and repairs initiated within seventy-two (72) hours. (i) If a dedicated camera malfunctions, alternative security procedures, such as additional supervisory or security agents, must be implemented immediately. (ii) The TGRA must be notified of any surveillance system and/or camera(s) that have malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented.	**Intent:** The control reduces potential risks to assets by discovering, documenting, reporting and addressing malfunctions of the surveillance system in a timely manner, and providing additional personnel and/or equipment to safeguard the assets in the event a dedicated camera malfunctions. **Testing:** 1. Review TICS and/or SICS to determine whether controls ensure the surveillance system is inspected periodically; malfunctions and repairs are documented and the TGRA is notified of malfunctions lasting more than 24 hours in duration are established and implemented. 2. Determine whether "alternative security procedures" in the case of a dedicated camera malfunction are included in the TICS or SICS for other gaming operation departments such as Security or Gaming. 3. Interview appropriate personnel (e.g., Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to— a. Determine how often surveillance system checks are completed and how those checks are logged. b. Determine who is responsible for conducting periodic inspections, and what the inspection includes. c. Discuss what "alternative security procedures" occur if there is a dedicated camera malfunction. d. Determine if alternative security procedures are included in the SICS for other gaming operation departments such as Security or Gaming. e. Determine how the TGRA is notified, and who at the TGRA is notified in the event of a malfunction that lasts more than 24 hours. 4. Review supporting documentation (e.g., Daily Activity Reports, Camera Check reports, and Malfunction/Repair Logs) to verify that malfunctions and necessary repairs have been documented

Citation	Language	Intent and Testing
		(see 543.21(f)(2)). Confirm that the repairs are initiated within 72 hours of being discovered. 5. Review documentation of notification being made to the TGRA of malfunctions lasting more than 24 hours in duration, and confirm that alternative security procedures that were taken. **Note:** 1. While dedicated camera malfunctions are specifically addressed in this control, note that the intent is to address "surveillance system" malfunctions generally. The surveillance system includes all equipment used for surveillance (*e.g.*, monitors, recording devices, selectors, switches, servers, cabling, patch panels, etc.). The requirements of this control therefore extends to periodic inspections, documentation of malfunctions, and notifications to the TGRA for all surveillance system equipment. **Best Practice:** 1. Require checks of all cameras at least once per shift and documenting the results. These results can be logged on the daily activity report log, or included with the storage, identification, and retention compliance log (see 543.21(f)(1)). Document any malfunction notifications to the TGRA, along with the date/time of the malfunction, date/time of notification, who was notified, how they were notified, and what alternative security measures were implemented. ("Alternative security measures" may involve the repositioning of a PTZ camera, the installation of a backup replacement camera, or the positioning of additional supervisory or security agents on the gaming floor to observe the activity being monitored by the dedicated camera.)

Citation	Language	Intent and Testing
543.21(c)(1)(i)-(ii)	(c) *Additional surveillance requirements*. With regard to the following functions, controls must also include: (1) Surveillance of the progressive prize meters for Class II gaming systems at the following thresholds: (i) Wide area progressives with a reset amount of $1 million; and (ii) In-house progressives with a reset amount of $250,000.	**Intent:** To deter, detect, and/or document potential misappropriation of assets or compromise to the integrity of Class II gaming systems, by requiring surveillance of high value prize meters. Additionally, recording of the meters protects the operation from potential liability and or fraud and abuse. **Testing:** 1. Review TICS to determine the controls for display and recording of required camera views are established and implemented. 2. Interview appropriate personnel (*e.g.,* Bingo Management, Surveillance Management, etc.) to determine which Class II gaming systems, if any, meet the threshold for wide area progressives with a reset amount of $1 million and in-house progressives with a reset amount of $250,000. 3. Observe the camera views of those Class II gaming systems meeting the progressive thresholds to verify that the camera can view the progressive prize meter and can be displayed on a monitor. 4. Observe the camera view recordings of those Class II gaming systems meeting the progressive thresholds to verify that the camera views are being recorded and retained for at least 7 days. **Note:** 1. Wide Area gaming machine contracts and or agreements should be reviewed for potential additional requirements that could be more stringent than the MICS.
543.21(c)(2)(i)-(ii)	(2) Manual bingo: (i) For manual draws, the surveillance system must monitor the bingo ball drawing device or mechanical random number generator, which must be recorded during the course of the draw	**Intent:** To protect the integrity of manual bingo games and to deter, detect, and/or document potential fraud or cheating in Class II manual bingo by requiring surveillance to monitor the ball drawing/number selection device and bingo activities.

Citation	Language	Intent and Testing
	by a dedicated camera to identify the numbers or other designations drawn; and (ii) The surveillance system must monitor and record the activities of the bingo game, including drawing, and entering the balls, numbers or other designations drawn.	**Testing:** 1. Review TICS to determine whether controls for display and recording of required camera views are established and implemented. 2. Interview appropriate personnel (*e.g.,* Bingo Management, Surveillance Management, etc.) to determine all locations where Bingo games are played, where Bingo equipment is located, and what Bingo games are played. 3. Observe the camera views of the manual bingo ball drawing device or mechanical random number generator to verify that the camera views can be displayed on a monitor and that a dedicated camera is used. Observe the camera view recordings to verify that they are being recorded during the course of the draw, and the recordings are retained for at least 7 days. 4. Observe the camera views of the activities of the bingo game, including drawing and entering the balls, numbers, or other designations drawn to verify that the camera views can be displayed on a monitor. Observe the camera view recordings to verify that they are retained for at least 7 days. **Notes:** 1. If other bingo games (*e.g.,* Bonanza, U-pick-em games, etc.) are played, verify that the required camera views are available for these game components (*e.g.,* bingo board, blower/hopper, U-pick-em boxes, etc.). 2. Additional MICS requirements include establishing TICS and implementing SICS for surveillance camera coverage with sufficient clarity to "identify persons accessing" the Bingo card inventory storage area, destruction of Class II gaming system components, and, while not specifically included in this control, coverage with sufficient clarity to "identify persons accessing" the pull tabs inventory storage area (see 543.8(b)(3)(i), 543.8(h)(2)(v)(B), and 543.9(b)(5)). For a definition of Class II gaming see 25 U.S.C. 2703(7)(A). 3. The coverage should be of sufficient clarity to identify the ball numbers drawn.

Citation	Language	Intent and Testing
543.21(c)(3) (i) (A)-(C), (ii)	(3) Card games: (i) Except for card game tournaments, a dedicated camera(s) with sufficient clarity must be used to provide: (A) An overview of the activities on each card table surface, including card faces and cash and/or cash equivalents; (B) An overview of card game activities, including patrons and dealers; and (C) An unobstructed view of all posted progressive pool amounts. (ii) For card game tournaments, a dedicated camera(s) must be used to provide an overview of tournament activities, and any area where cash or cash equivalents are exchanged.	**Intent:** To protect the integrity of the card games and tournaments and to deter, detect, and/or document potential theft, cheating, or misappropriation of assets within them by requiring surveillance to record individuals and activities. **Testing:** 1. Review TICS to determine whether controls, which provide for display and recording of required camera views are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine how often card game tournaments occur, where they occur, and how long they occur. 3. For card games— a. Observe the required camera views of (1) the activities on each card table surface (card faces and/or cash equivalents), (2) an overview of card game activities (patrons and dealers), and (3) all posted progressive pool amounts. b. Verify that the card game camera views can be displayed on a monitor, and that a dedicated camera is utilized. c. Observe the recordings for card game activities to verify that they are being recorded and retained for at least 7 days, and that they are recorded with sufficient clarity (20 fps and with resolution sufficient to clearly identify the intended person, activity, object, or location). 4. For card game tournaments-- a. Observe the required views of an overview of tournament activities and any area where cash or cash equivalents are exchanged. b. Verify that the camera views can be displayed on a monitor, and that a dedicated camera is used. c. Observe the required camera view recordings to verify that they are being recorded and retained for at least 7 days.

Citation	Language	Intent and Testing
		Best Practices: 1. The MICS only designate certain camera views as requiring "sufficient clarity." Therefore, the TICS and SICS should identify whether additional camera views (as determined by the Tribe/TGRA) that are important to the effective regulation and protection of the Tribe's gaming activities. These additional camera views should also be designated in the SICS and TICS as requiring "sufficient clarity." **Notes:** 1. Additional MICS requirements include establishing TICS and implementing SICS for surveillance camera coverage of the secure location where new and used playing cards are maintained and destruction of Class II gaming system components (see 543.10(c)(1) and 543.8(h)(2)(v)(B)). For a definition of Class II gaming see 25 U.S.C. 2703(7)(A)). 2. Sufficient clarity and dedicated camera are terms with specific meanings, which may be found in the Glossary and in 25 C.F.R. §543.2
543.21(c)(4)(i)-(iii)	(4) Cage and vault: (i) The surveillance system must 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 transaction; (ii) Each cashier station must be equipped with one (1) dedicated overhead camera covering the transaction area; and (iii) The cage or vault area in which exchange and transfer transactions occur must be monitored and recorded by a dedicated camera or motion activated dedicated camera that provides	**Intent:** To deter, detect, and/or document potential misappropriation of assets, by identifying individuals and activity, confirm the amount of transactions, and to document compliance with applicable internal control standards. **Testing:** 1. Review TICS to determine whether controls, which provide for display and recording of required camera views are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine where all cage and vault areas are located. Determine whether there are any satellite cage areas. Determine

Citation	Language	Intent and Testing
	coverage with sufficient clarity to identify the chip values and the amounts on the exchange and transfer documentation. Controls provided by a computerized exchange and transfer system constitute an adequate alternative to viewing the amounts on the exchange and transfer documentation.	the process for monitoring exchanges and transfers occurring in the cage or vault areas. 3. Observe the required camera views of the general overview of activities occurring in each cage and vault area. Verify that the camera views can be displayed on a monitor, that they are being recorded and retained for at least 7 days. Verify the camera views are recorded with sufficient clarity, *i.e.,* 20 fps and with resolution sufficient to clearly identify individuals within the cage, patrons and staff members at the counter areas, and the amount of each cash transaction). 4. Observe the required camera views of each cashier station in each cage and vault area (subsection (ii)). Verify that the camera views can be displayed on a monitor, that they are being recorded and retained for at least 7 days, and that a dedicated camera is utilized. 5. Observe the required camera views of the cage and vault area in which exchange and transfer transactions occur. Verify that the camera views can be displayed on a monitor and that a dedicated camera or motion-activated camera is utilized. Also, verify that camera views are being recorded and retained for at least 7 days, and that they are recorded with sufficient clarity, *i.e.*, 20 fps and with resolution sufficient to clearly identify chip values and the amounts on the exchange and transfer documentation (if not computerized). **Notes:** 1. Sufficient clarity and dedicated camera are terms with specific meanings, which may be found in the Glossary and in 25 C.F.R. § 543.2. 2. The requirement to "confirm the amount of each cash transaction" implies that the camera view should be sufficiently clear to observe the denominations of any cash and cash equivalents exchanged, and the observer be able to determine the details of the transaction. 3. Multiple cameras may be required in order to obtain adequate camera views to identify individuals within the cage, patrons and

Citation	Language	Intent and Testing
		staff members at the counter areas, and to confirm the amount of each cash transaction as required. 4. An alternative procedure offered in the minimum internal control states: "Controls provided by a computerized exchange and transfer system constitute an adequate alternative to viewing the amounts on the exchange and transfer documentation." However, if this alternative control is used, the chip values must still be visually observed and compared to the amounts on the computerized exchange and transfer system documentation. In addition, TGRA approved SICS must be established and implemented.
543.21(c)(5) (i)-(ii)	(5) Count rooms: (i) The surveillance system must monitor and record with sufficient clarity a general overview of all areas where cash or cash equivalents may be stored or counted; and (ii) The surveillance system must provide coverage of count equipment with sufficient clarity to view any attempted manipulation of the recorded data.	**Intent:** To deter, detect, and/or document potential misappropriation of assets, by creating an additional independent record of the amount of transactions. **Testing:** 1. Review TICS to determine whether controls, which provide for display and recording of required camera views are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine all areas where "cash or cash equivalents may be stored or counted." Determine by inquiry a general description of the count process, and any count procedures that require the involvement of Surveillance (*e.g.,* showing empty drop boxes to Surveillance). 3. Observe the required camera views of the count rooms, a general overview of all areas where cash or cash equivalents may be stored or counted, and the count equipment. Verify that the camera views can be displayed on a monitor, that they are being recorded and retained for at least 7 days, and that they are recorded with sufficient clarity to view any attempted manipulation of the data.

Citation	Language	Intent and Testing
		Notes: 1. Sufficient clarity is a term with specific meaning, which may be found in the Glossary and in 25 C.F.R. § 543.2. 2. Additional MICS requirements include the notification to Surveillance agents whenever count room agents exit or enter the count room during the count (see 543.17(b)(2)). Notification when the drop begins so Surveillance agents can monitor the activities (see 543.17(d)(1) and 543.17(e)(1)). Notification when emergency drops are required (see 543.17(d)(5) and 543.17(e)(3)). These notifications are typically documented on the Surveillance Department daily activity log or call log.
543.21(c)(6)	(6) Kiosks: The surveillance system must monitor and record a general overview of activities occurring at each kiosk with sufficient clarity to identify the activity and the individuals performing it, including maintenance, drops or fills, and redemption of wagering vouchers or credits.	**Intent:** To deter, detect, and/or document potential misappropriation of assets by monitoring activity and the individuals performing maintenance, drops or fills, and redemption of wagering vouchers and credits. **Testing:** 1. Review TICS to determine whether controls for display and recording of required camera views are established and implemented. 2. Observe the required camera views of the general overview of activities occurring at each kiosk. Verify that the camera views can be displayed on a monitor, and that they are being recorded and retained for at least 7 days. Verify the camera views are recorded with sufficient clarity to identify the activity and the individuals performing it (including maintenance, drops and fills, and redemption of wagering vouchers or credits). **Notes:** 1. Sufficient clarity is a term with specific meaning, which may be found in the Glossary and in 25 C.F.R. § 543.2. It may require more than one camera per kiosk to obtain both a general overview of activities at each kiosk and a view sufficient to "identify the activity and the individuals performing it."

Citation	Language	Intent and Testing
543.21(d)	(d) *Reporting requirements*. TGRA-approved procedures must be implemented for reporting suspected crimes and suspicious activity.	**Intent:** To protect the integrity, assets, and safety of the gaming operation, its patrons and employees by reporting suspected crimes and suspicious activity consistent with methods approved by the TGRA. **Testing:** 1. Review SICS to determine whether controls for reporting suspected crimes and suspicious activity are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine the procedure for reporting suspected crimes and suspicious activity. 3. Locate written documentation of TGRA approval for reporting suspected crimes and suspicious activity. 4. Review documentation of a recent example of reporting suspected crime and suspicious activity. Verify that the document describes who the activity was reported to, how it was reported, and in what timeframe it was reported. **Best Practices:** 1. Surveillance should have procedures describing what constitutes a "suspected crime or suspicious activity" and detail specifically a. Who the activity is reported to, b. How it is reported (*e.g.*, phone, email, text, etc.), and in what timeframe notification is to be made.
543.21(e)(1)	(e) *Recording retention*. Controls must be established and procedures implemented that include the following: (1) All recordings required by this section must be retained for a minimum of seven days; and	**Intent:** To allow a reasonable amount of time for concerns to be raised and initiate a review of the recordings without requiring overly burdensome storage capacity. **Testing:** 1. Review TICS and/or SICS to determine whether controls for retaining the required recordings at least seven days are established and implemented.

Citation	Language	Intent and Testing
		2. Review video recordings or system logs that document the number of days required recordings are being retained. Note the length of time indicated for recording retention. 3. Observe samples of recorded video to verify that required recordings are retained a minimum of seven days as required. **Best Practices:** 1. Each TGRA/operation should determine its own needs for video recording retention. While the minimum control requirement is retention of recorded video for at least seven days, many operations prefer to require retention for at least thirty days finding that the additional time better meets their needs. 2. In determining a recording retention period beyond the seven-day minimum, consider the time needed for the Surveillance Department to receive the request as well as the time needed to retrieve and copy the video.
543.21(e)(2)	(2) Suspected crimes, suspicious activity, or detentions by security agents discovered within the initial retention period must be copied and retained for a time period, not less than one year.	**Intent:** To protect the assets, integrity, and safety of the tribal gaming operation by requiring preservation of video documentation that may be used as evidence to extend beyond the initial retention period. **Testing:** 1. Review TICS and/or SICS to determine whether controls for copying recordings of "suspected crimes, suspicious activity, or detentions by security agents" and retention for at least one year are established and implemented. 2. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to determine the procedure for retaining recorded video of suspected crimes, suspicious activity, or detentions by security agents. Determine by what method recorded video is maintained and for what length of time it is retained (minimum time period is one year).

Citation	Language	Intent and Testing
		3. Review video recordings or system logs that document how long required video recordings are retained. Document the length of time that copied video is retained. 4. Observe samples of video to verify recordings are retained for at least one year. **Best Practices:** 1. Video recordings of "suspected crimes, suspicious activity, or detentions by security agents" should be copied to more permanent recording mediums, *e.g.,* DVD's, CD's, flash drives, or segregated digital recording space on a server. This allows for a more permanent preservation of video recordings that may be used as evidence or for training. Additionally, it is recommended recordings of incidents be saved and retained in proprietary format to be preserved as evidence to ensure against allegations of tampering. **Notes:** 1. While the minimum control requirement is retention of recorded video for at least one year, recording retention may need to be increased in order to meet the particular needs of the gaming operation, surveillance operation, and Tribe. 2. Recordings of "suspected crimes, suspicious activity, or detentions by security agents" may be used as evidence in legal or other formal proceedings (*e.g.*, criminal prosecutions, insurance cases, human resource matters, etc.).
543.21(f)(1)	(f) *Logs*. Logs must be maintained and demonstrate the following: (1) Compliance with the storage, identification, and retention standards required in this section;	**Intent:** To ensure surveillance maintains a log, which documents compliance with the storage (Electronic and or other medium for video recording), identification, and retention standards, as required. **Testing:** 1. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to confirm logs are maintained which demonstrate

Citation	Language	Intent and Testing
		compliance with the storage, identification, and retention standards required. (Best practices indicate that a log should be completed and maintained on a routine basis, either weekly, daily, or at the beginning of each shift. The log may be a paper log, a computer log, or a computer-generated report from the digital video recording system.) 2. Review logs to verify that they document compliance with storage, identification, and retention standards required. Verify that the logs are being retained for at least five years (see part 571.7(c)). 3. Due to many surveillance systems going to a digital format, some surveillance departments utilize their daily activity log to maintain compliance with this standard. If utilizing the daily activity log, the surveillance department should be diligent in recording accurate dates and times of activity to ensure the appropriate video can be accessed when necessary. Additionally, some surveillance departments use daily activity logs to perform camera and recorder checks for clarity and retention. When that is practiced, it is recommended the results of these checks be properly documented in the activity log. **Notes:** 1. Compliance is achieved for this control by documenting that the storage, identification, and retention standards in Part 543.21 are being met. Storage refers to the required camera views being recorded – "Are the required camera views being recorded?" Identification refers to the ability to be able to clearly identify an activity, person, object, or location; as detailed in the Sufficient Clarity requirement and definition – "Are the required camera views being recorded at a minimum of twenty (20) frames per second (or equivalent), and at a resolution that is sufficient to clearly identify the intended activity, person, object, or location?" Retention refers to keeping required camera view recordings for a minimum of seven (7) days – "Are required camera view recordings retained for a minimum of at least seven days?"

Citation	Language	Intent and Testing
		2. While documentation of compliance with the identification standards related to "sufficient clarity" includes the number of frames per second of recording rate, it is important to note that also included in the definition of "sufficient clarity" is the requirement that resolution is sufficiently clear as well to identify the intended activity, person, object, or location. This means that although the recording framerate is at least 20 frames per second, resolution must also be sufficient so that the video is clear enough during playback to identify the object of the surveillance.
543.21(f)(2)	(2) Each malfunction and repair of the surveillance system as defined in this section; and	**Intent:** To ensure that surveillance malfunctions are made known and repaired in a timely fashion. In addition, to document a history of the system that can be reviewed for unusual activity. **Testing:** 1. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to confirm logs are maintained that document each malfunction and repair of the surveillance system. 2. Review logs to verify that they document each malfunction and repair of the surveillance system. Verify that the logs are being retained for at least five years (see part 571.7(c)). Also, verify that TGRA notification is occurring and that alternative procedures are implemented (see 543.21(b)(11)(ii)). **Best Practices:** 1. The log should state-- a. The time, date, and nature of each malfunction, b. The efforts expended to repair the malfunction, c. The date of each effort, the reasons for any delays in repairing the malfunction, the date the malfunction is repaired, and d. Any alternative security measures that were taken (if applicable). e. When TGRA notified, how was notification made. *i.e.,* phone, email.

Citation	Language	Intent and Testing
543.21(f)(3)	(3) Activities performed by surveillance agents as required by the controls in this section.	**Intent:** To ensure that TICS and SICS are established and implemented that provide a level of control that equals or exceeds the MICS requirement for the maintaining of a log (or logs) which documents the activities required by the controls in this section performed by surveillance agents. **Testing:** 1. Interview appropriate personnel (*e.g.,* Surveillance Manager/Director, Surveillance Shift Manager/Lead, Surveillance Agent) to confirm logs are maintained that document activities performed by surveillance agents as required by the controls in this section. 2. Review logs to verify that they document activities performed by surveillance agents as required by the controls in this section (see Notes). Verify that the logs are being retained for at least five years (see part 571.7(c)). **Best Practices:** 1. Establish the log requirement in writing either as a TICS or SICS. 2. A log should be maintained that, at a minimum, records the following information: a. Date, time commenced and terminated, b. Activity observed or performed, and c. The name or license credential number of each person who initiates, performs, or supervises the surveillance. 3. The log should include a summary of the results of the surveillance of any suspicious activity. **Notes:** 1. The following activities are required by the controls of this section and should be documented in the surveillance activities log: a. Suspected crimes, suspicious activity, or detentions by security agents, b. Individuals accessing the surveillance operation room(s), c. Exchange and transfers,

Citation	Language	Intent and Testing
		d. Drop and count activities, and e. Maintenance, dropping, and filling of the kiosks.

Additional Relevant Standards Outside of §543.21

Citation	Language	Intent and Testing
543.8(b)(3)(i)	(b) *Bingo Cards*. (3) Storage (i) Bingo cards must be maintained in a secure location, accessible only to authorized agents, and with surveillance coverage adequate to identify persons accessing the storage area.	**Intent:** To reduce potential misappropriation of assets or compromise to the bingo game by providing for a secured location to store bingo cards with proper surveillance coverage. **Testing:** 1. Interview appropriate personnel (*e.g.,* Bingo Management, Surveillance Management, etc.) to determine all locations where Bingo cards are stored and what Bingo games are played. 2. Review TICS and/or SICS to determine if procedures have been implemented that specify who the authorized agents are and identify the secure location. 3. Observe the camera views of the bingo storage location to verify that the camera views can be displayed on a monitor and that a dedicated camera is used. Observe the camera view recordings to verify that they are being recorded and the recordings are retained for at least 7 days. 4. Observe the camera views of the bingo storage access and bingo storage access logs to verify that only authorized agents are accessing the inventory. Observe the camera view recordings to verify that they are retained for at least 7 days.
543.8(h)(1)(ii)	(h) *Operations*. (1) Malfunctions. Procedures must be implemented to investigate, document and resolve malfunctions. Such procedures must address the following: (ii) Review of relevant records, game recall, reports, logs, surveillance records;	**Intent:** To ensure the integrity of the bingo game by implementing procedures to investigate, document and resolve malfunctions, review of available documentation of the malfunction, repair or replacement if needed and verification of the system component's integrity prior to restoring to operation. **Testing:** 1. Review TICS and or SICS to determine if procedures have been created addressing malfunctions investigation steps and documentation requirements. If surveillance is part of the

Citation	Language	Intent and Testing
		malfunction investigation process, then the TICS and/or SICS should identify the surveillance records that are authorized to be provided. 2. Review if applicable a sample of malfunction, repair and replacement records. (Look at sample as defined in the Glossary) 3. Interview appropriate personnel to verify malfunction procedures if no sample to test. (*e.g.,* Bingo Management, Bingo personnel)
543.8(h)(2)(v)(B)	(h) *Operations*. (2) Removal, retirement and/or destruction (v) Where the TGRA authorizes destruction of any Class II gaming system components, procedures must be developed to destroy such components. Such procedures must include the following: (B) Witness or surveillance of destruction;	**Intent:** To prevent potential misappropriation of assets and ensure the integrity of the bingo game by implementing procedures for removal, retirement and destruction of Class II gaming system components to include witnessing destructions. **Testing:** 1. Interview appropriate personnel (*e.g.,* TGRA, Bingo Management, Surveillance Management, etc.) to determine whether destruction of class II components is authorized. 2. Review TICS and/or SICS to determine if procedures have been implemented that specify whether destruction must be witnessed live or by surveillance. 3. Observe the camera views of the location where bingo system components are destroyed to verify that the camera views can be displayed on a monitor and that a dedicated camera is used. Observe the camera view recordings to verify that they are being recorded and the recordings are retained for at least 7 days, or longer if required by the TICS and/or SICS. **Note:** 1. Most class II system components are leased, so if the vendor is responsible for the removal, retirement, and/or destruction processes, then the SICS should explicitly state the vendor is responsible for those processes.

Citation	Language	Intent and Testing
543.9(b)(5)	(b) *Pull tab inventory.* Controls must be established and procedures implemented to ensure that: (5) Pull tabs are maintained in a secure location, accessible only to authorized agents, and with surveillance coverage adequate to identify persons accessing the area.	**Intent:** To reduce potential misappropriation of assets or compromise to the pull tab games by providing for a secured location to store pull tabs with proper surveillance coverage. **Testing:** 1. Interview appropriate personnel (*e.g.,* Pull Tabs Management, Surveillance Management, etc.) to determine all locations where pull tabs are stored and what pull tab games are played. 2. Review TICS and/or SICS to determine if procedures have been implemented that specify who the authorized agents are and identify the secure location. 3. Observe the camera views of the pull tab storage location to verify that the camera views can be displayed on a monitor and that a dedicated camera is used. Observe the camera view recordings to verify that they are being recorded and the recordings are retained for at least 7 days. 4. Observe the camera views of the pull tab storage access and pull tab storage access logs to verify that only authorized agents are accessing the inventory. Observe the camera view recordings to verify that they are retained for at least 7 days.
543.10(c)(1)	(c) *Playing cards*. (1) New and used playing cards must be maintained in a secure location, with appropriate surveillance coverage, and accessible only to authorized agents.	**Intent:** To reduce potential misappropriation of assets or compromise to the card games by providing for a secured location to store new and used playing cards with proper surveillance coverage. **Testing:** 1. Interview appropriate personnel (*e.g.,* Card Games Management, Surveillance Management, etc.) to determine all locations where playing card are stored before and after use. 2. Review TICS and/or SICS to determine if procedures have been implemented that specify who the authorized agents are and identify the secure location.

Citation	Language	Intent and Testing
		3. Observe the camera views of the playing card storage location to verify that the camera views can be displayed on a monitor and that a dedicated camera is used. Observe the camera view recordings to verify that they are being recorded and the recordings are retained for at least 7 days. 4. Observe the camera views of the playing card storage access and card storage access logs to verify that only authorized agents are accessing the inventory. Observe the camera view recordings to verify that they are retained for at least 7 days. **Note:** 1. If used playing cards are stored in a room prior to being marked or destroyed, then surveillance of that room must be included in these requirements. Additionally, some SICS require surveillance to observe the marking or destruction of used playing cards so surveillance operations should be mindful of those requirements.
543.20(b)	(b) As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.	**Intent:** Computerized 'systems' are defined as computerized systems integral to the operation of the gaming environment. Systems include electronic/electrical networked-system environments, and the surveillance system is defined as part of the Class II system. **Testing:** 1. Review gaming operations architectural plans and computerized network system design layout and applications system inventory.

5 CFR 543.21 Toolkit

Version 1.0

NIGC Division of Public Affairs

National Indian Gaming Commission

Training Manager
Training Program