NATIONAL INDIAN GAMING COMMISSION

Participant Workbook
Portland RGT Conference
February 27-28, 2018

Dear Training Course Participant,

Over twenty five years ago Congress adopted the Indian Gaming Regulatory Act (IGRA) to provide statutory support for gaming by Indian tribes. The National Indian Gaming Commission (NIGC) was created by IGRA to partner with tribal regulators to regulate gaming activities conducted by sovereign Indian tribes on Indian lands. The mission of the NIGC is to fully realize IGRA's goals of: (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.

One of the primary ways the NIGC does this is by providing training and technical assistance to Indian tribes and their gaming regulators.

A properly trained and informed workforce is the most successful key to regulation and the assurance of compliance. Focused, targeted and responsive training and technical assistance programs provide a foundation that maintains the integrity and success of Indian gaming.

Through dedication and hard work, Indian gaming has experienced notable and successful growth thanks to the partnership of dedicated employee's, regulators and tribal governments and the NIGC. Our continued success depends on grabbing the growing momentum and "*Work Together for Success*", now and into the coming future.

With this backdrop in mind, we encourage you to take advantage of the NIGC training opportunities highlighted by this course. The Commission recognizes your work is essential to the success of Indian gaming and encourages you to use the tools you will receive and knowledge you will gain from this course to further regulatory excellence in Indian gaming.

Jonodev Osceola Chaudhuri
NIGC Chairman

Kathryn Isom-Clause
Associate Commissioner

E. Sequoyah Simermeyer
Associate Commissioner

Course Rationale

The National Indian Gaming Commission (NIGC) RGTCourse is designed to provide a common foundation of knowledge and skills to prepare Tribes to work together to effectively understand and meet requirements to ensure compliance and provide a successful basis for economic development.

NIGC Training is built around adult learning principles, with knowledge delivery for understanding and everywhere possible, application level exercises, workshops and opportunities to collaborate in or for each attendee to have an opportunity to achieve understanding, doing and getting feedback on results – and doing again! Working together and using the skills and knowledge applicable to improve processes as soon as they return to work.

The 6 key benefits to the NIGC Training Model:

1. Provides real focus on issues and concerns important to attendees for meeting compliance.
2. Builds a sense of shared experience and language around the tools and methodologies.
3. Develops an understanding of the trends and concerns impacting Tribes and Indian Country in gaming.
4. Provides a safe environment for query, experimentation and failure.
5. Encourages application and testing in a true problem solving focus.
6. Provides a venue to develop relationships that improve communication, commitment and productivity.

Course Descriptions

The National Indian Gaming Commission (NIGC) RGT course is designed to provide an advanced knowledge of skills to prepare all staff to work together to effectively understand and meet requirements. Gaming staff that have been working in the gaming industry are in need of training to stay current with advances in technology within the gaming environment. The NIGC RGT course creates a learning environment in which staff will have the opportunity to learn about and gain knowledge of the roles, responsibilities, hardships, and challenges that staff in every position, from commissioners to a variety of others in attendance encounter.

NIGC's targeted training will provide instruction in areas such as the verification of Class II gaming machines, the technical standards required to be in compliance, gaming forensics and auditing to 543.20. Training will include an emphasis on compliance and professional development in all subjects. Improved staff capability and knowledge will directly impact both the staff member and their program organizational climate.

IT – 113 IT Basics

A learning block designed for tribal gaming regulators, operations and IT personnel that desire basic gaming and Information Technology knowledge. The objective of this lesson is to gain a basic understanding of Information Technology and gaming terminology, being able to differentiate between Class II and Class III gaming machines. You will gain an understanding of gaming and Information Technology at a beginning level to set a foundation for understanding the IT courses taught at the RGT.

IT – 110 Refining and Enhancing Your IT TICS

A learning block designed for tribal gaming regulators, operational and IT personnel. Due to the ever changing IT world this course will explore common technical concerns of gaming regulators. This course is intended as a prequel to the IT Auditing 543 and should help provide some reassurance regarding creating and maintaining IT TICS. Lastly it will explore techniques for reviewing, revisiting and improving IT TICS to better suit your operations.

IT – 109 Auditing 543

A learning block designed for tribal gaming regulators, operational and IT personnel. It will explore the 25 C.F.R. Part 543.20 Minimum Internal Control Standards for Class II Gaming. We will discuss during a typical IT audit commonly identified problem areas and how to apply relevant best practices for overcoming the recognized concerns. Utilizing real world examples we will highlight various MICS and emphasize common IT compliance issues.

IT – 112 System Verification & Game Authentication Tool

A learning block offered to tribal gaming regulators, operations and IT personnel. The course will focus on various systems verification tools and introduce attendees to game authentication method;: i.e. G2S and SAS protocols and the benefits for regulators.

Course Descriptions

IT – 108 IT Threats for Casinos

A learning block offered to tribal gaming regulators, operations and IT personnel. The course will focus on current and trending threats to IT systems and security within the technology framework in Casinos. i.e. ransomware, social engineering, and denial of service Focusing on threats, vulnerabilities and processes, this block will provide real time information on what risks exist and how best to combat them.

IT – 107 Gaming Forensics

A learning block offered to tribal gaming regulators, operations and IT personnel. It will explore different types of forensics in today's industry for example; a typical scenario of gaming or associated equipment malfunctioning or performing an operation outside the range of that equipment's programmed abilities. The course will review various strategies, best practices, and other guidelines available for regulators and tribal gaming personnel in dealing with equipment malfunctions and thefts.

How to Get the Most Out of This Course

- **Take the right approach to learning.** To meet each attendee's needs, we provide a number of different learning tools. These include well-researched and professionally prepared materials and presentations by skilled and experienced subject matter experts. Although you'll have a preferred style of learning, we hope you'll take advantage of *all* the tools we offer.

- **Make a note of this.** This workbook and related materials will enable you to take notes, and have access to needed information. Instead of trying to take notes word-for-word, it is recommended that you list key points for later memory jogging. We will try and ensure you have as much information as you need to lessen the need for lengthy notes.

- **Don't hesitate, participate.** The course will be more interesting and productive when everyone participates. If you don't understand something, there is a good chance someone else does not either, so do everyone a favor and ask questions. Additionally, don't hesitate to answer our questions and share your relevant knowledge and experience with all of us.

- **Take a break.** Everyone has a limit to how much they can sit still and absorb. So use the break, network, share ideas, and get some fresh air. You can help keep us running smoothly by coming back on time.

- **Join in with the group.** Stay enthusiastic and involved.

- **Attendance.** You must fully attend the course, and where applicable, pass a final exam for full credit and to receive a training certificate. Please do your best to be on time for class and try to be here for the entire course.

- **Cell phones, PDA's and iPad's.** In an effort to minimize disruptions to class, please turn off all cell phones and PDA's. If they are your only emergency contact, please set them to vibrate. IPad's may be used, but should be for note taking.

Please note: This course is conducted in English with instruction facilitated by verbal and written communications.

Course Structure

The Regulating Training Course is a 2 day course developed to provide an encompassing event surrounding current, trending and critical knowledge areas in Indian gaming. Providing full staff learning opportunities, as well as focus area learning tracks, the course is designed to give tribal gaming regulators and operations personnel, commissions and staff a wide variety of subject needs to meet concerns and relevant areas of interest in Indian gaming.

Each instruction topic is focused around identified concern areas, new content and regulations and a variety of mechanisms for change, improvement and compliance for success. Each block focuses on various staff roles and responsibilities, focusing on similarities, differences, and opportunities for collaboration and sharing of practices and improvements. Most topic areas will pair an equal amount of time to facilitated lecture and action based learning.

The primary training methodologies will be interactive lecture, small group discussion, and case study. Action based learning will be facilitated through small groups and case study. Final learning will be measured through exercise completion and observation.

Regulating Gaming Technology Agenda

	START TIME	PORTLAND REGIONAL GAMING TECHNOLOGY **February 27th – 28th, 2018** Snoqualmie Casino 37500 SE North Bend Way Snoqualmie, WA 98065
Day One	**08:30**	Course Opening/Welcome
	09:00	IT-113 IT Basics
	10:45	Break
	11:00	IT-110 Refining and Enhancing your IT TICS
	12:00	***Lunch (On your own)***
	1:00	IT-110 Refining and Enhancing your IT TICS
	1:45	Break
	2:00	IT-109 Auditing 543
	3:15	Break
	3:30	IT-109 Auditing 543
	4:30	**Q&A**
Day Two		**DAY TWO**
	8:30	IT-112 System Verifications & Authentication
	9:30	Break
	9:45	IT-112 System Verifications & Authentication
	10:45	Break
	11:00	IT-108 IT Threats
	12:00	***Lunch (On your own)***
	1:00	IT-108 IT Threats
	2:00	Break
	2:15	IT-108 IT Threats
	3:15	Break
	3:00	IT-107 Gaming Forensics
	4:30	**Course Close**

IT-113 Information Technology Basics

IT-113 Information Technology Basics Participant Guide

IT-113 Information Technology Basics

Information Technology Division

KEY POINTS

Knowledge Reviews & Course Evaluations

Knowledge Review Purpose

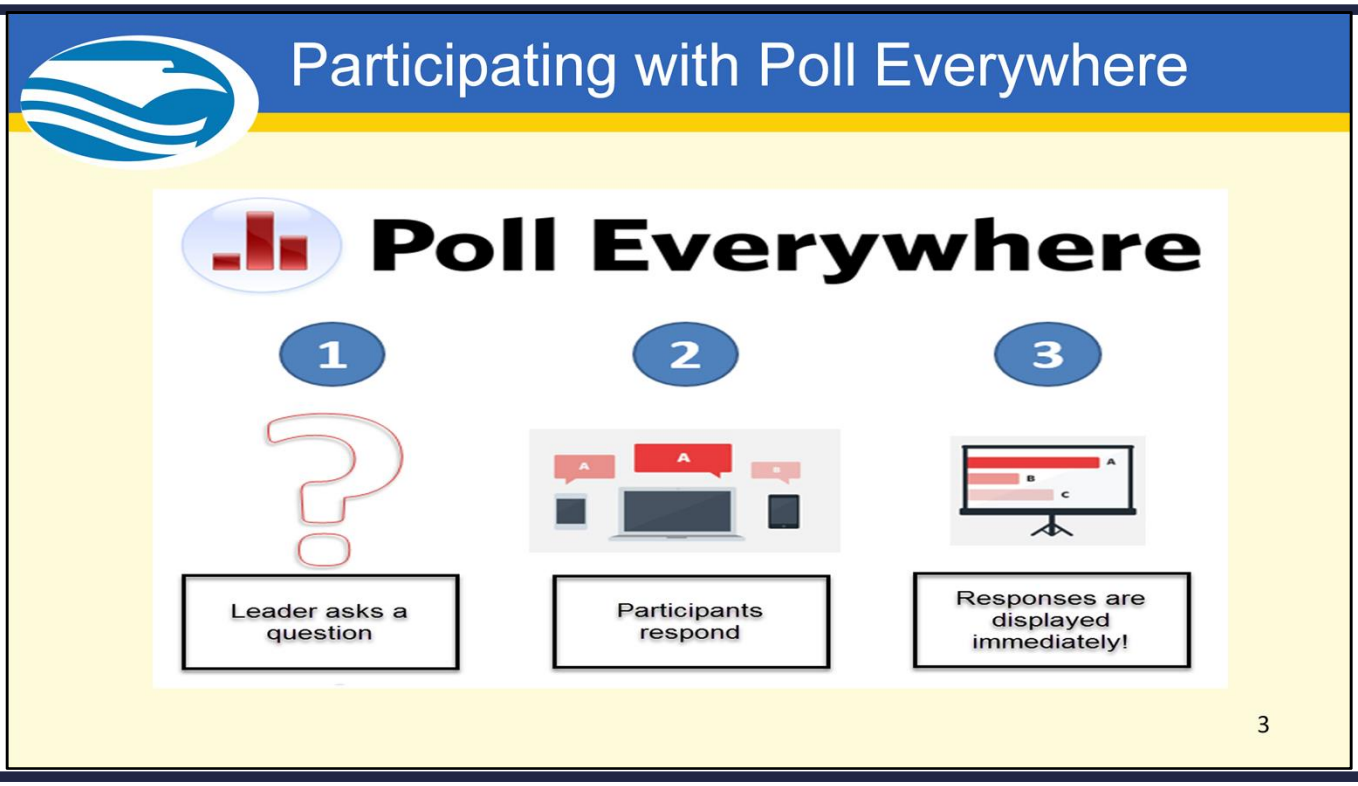
- Check for immediate understanding and retention
- Used to improve courses
- Provide your name & email address
- Completed twice:
  - at the end of the course
  - 90 days after course via email

Evaluation Purpose

- Allow participants to provide immediate feedback on their experience
- Encouraged to include ideas and recommendations
- Will be used to improve the course

2

KEY POINTS



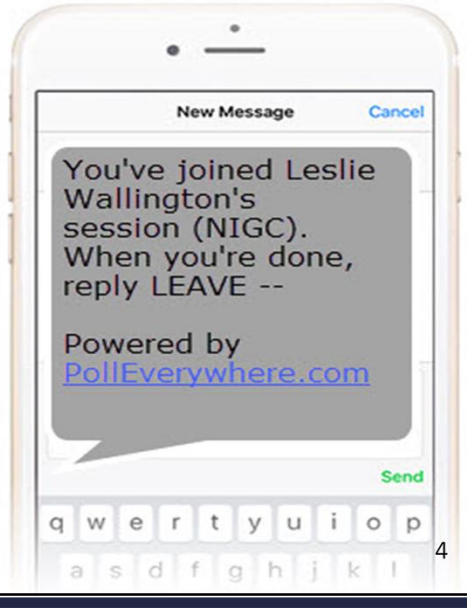
KEY POINTS

During the presentations we will be asking you polling question and we would you like to practice using the Poll Everywhere.

Your participation is voluntary and your responses are anonymous.

Response from Poll Everywhere

1. You will receive a text message confirming that you are in the polling session.
2. Do **NOT** select the PollEverywere.com link.
3. Now you can enter your response to the poll as a text message.



4

KEY POINTS

After your first text sent to 22333 you will receive a confirmation message.
Do NOT select the link included here.
Simply respond to the poll listed on the PowerPoint.

Using Your Phone to Participate

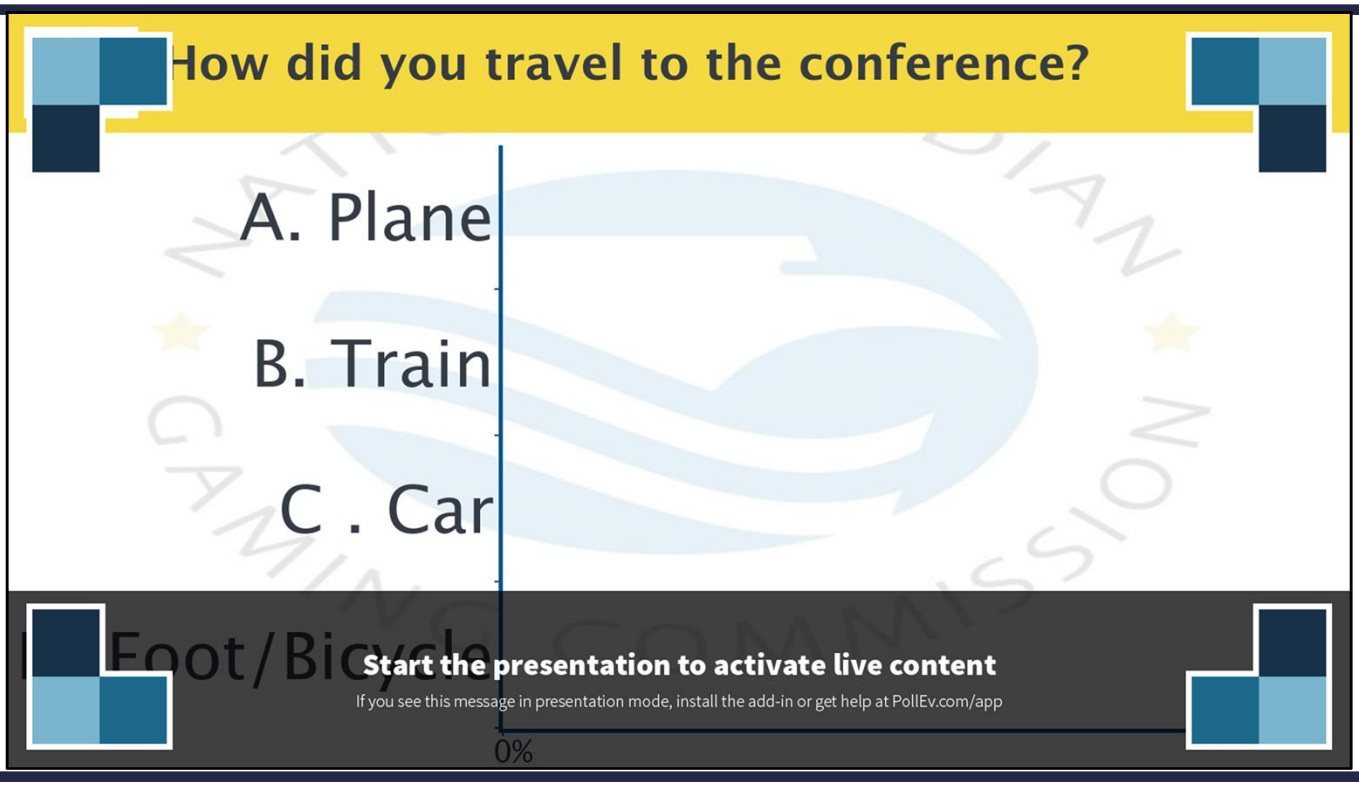
1. Text NIGC to 22333 to join the session.
2. Then text your response to the question: **How did you travel to the conference?**

A. Plane
B. Train
C. Car
D. Foot/Bicycle

5

KEY POINTS

1. Text **NIGC** to **22333** to join the session.
2. Then text your response to the question:



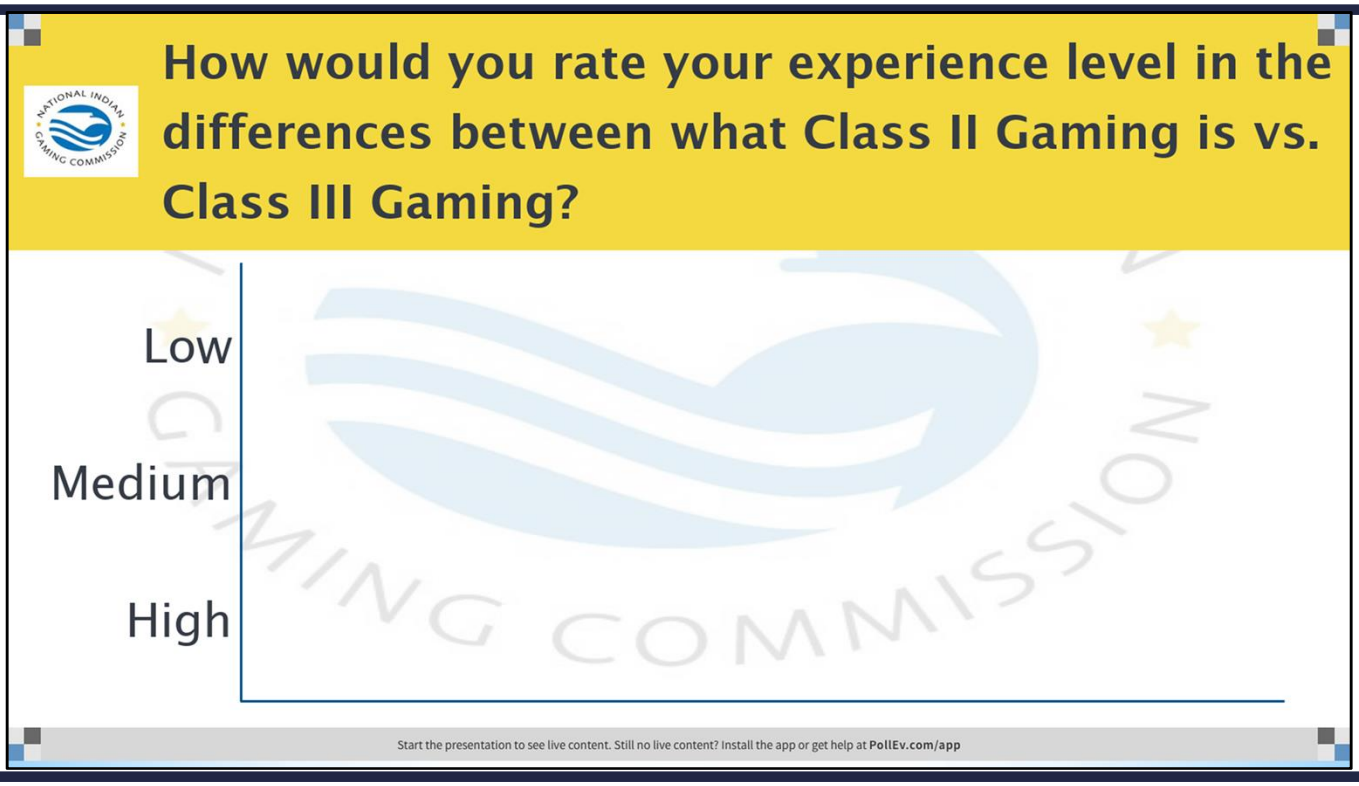
KEY POINTS

Poll Title: How did you travel to the conference?

https://www.polleverywhere.com/multiple_choice_polls/yldbms0zVYqpfn5

KEY POINTS

Poll Title: How would you rate your IT experience level in a Casino environment?
https://www.polleverywhere.com/multiple_choice_polls/EhU9Jx1JlRA08XR



KEY POINTS

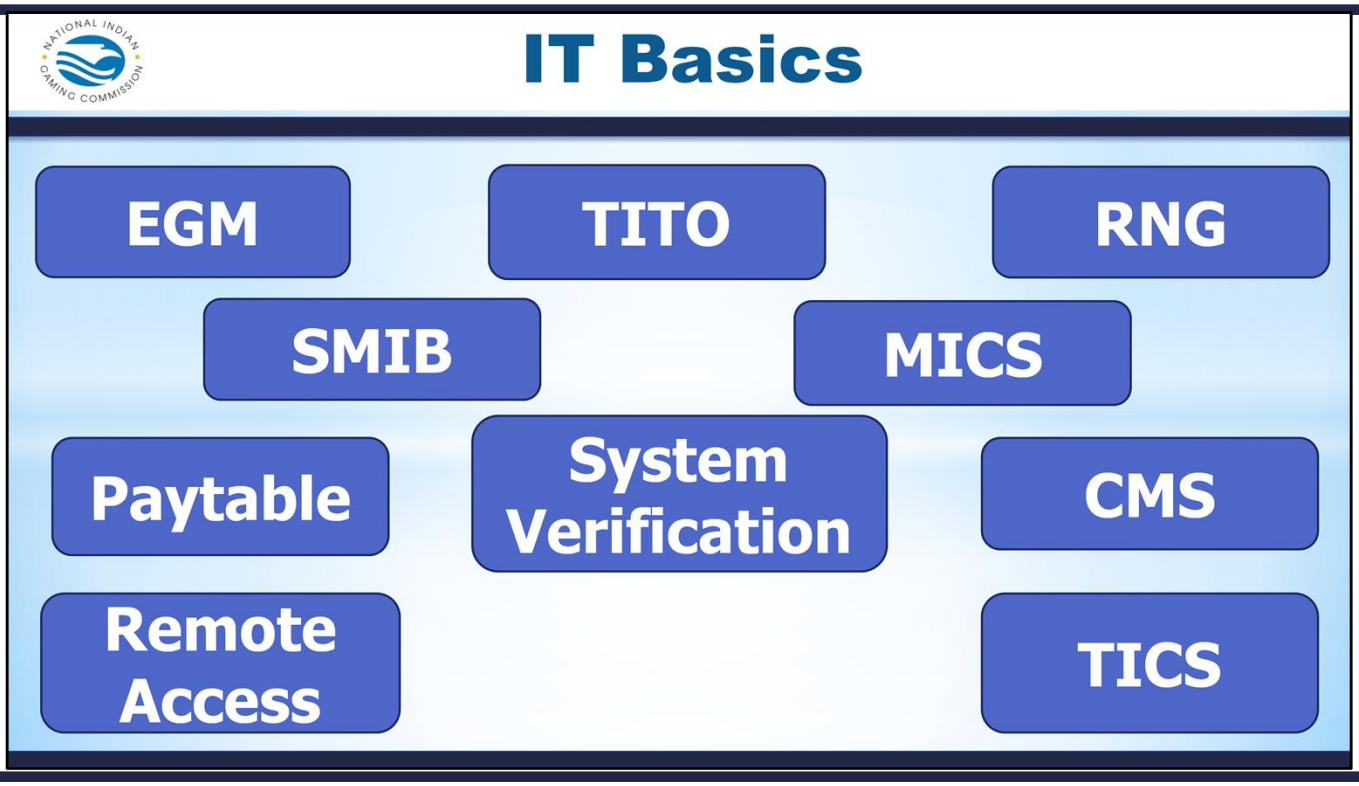
Poll Title: How would you rate your experience level in the differences between what Class II Gaming is vs. Class III Gaming?

https://www.polleverywhere.com/multiple_choice_polls/FtHi407GEQSvUiG

IT Basics - Overview

- Gaming Terminology
- Class II Review
- Class III Review
- Activity

KEY POINTS



KEY POINTS

1. EGM is used as a shorthand for "Electronic Gaming Machine."

2. RNG Random Number Generator All modern machines are designed using pseudo random number generators ("PRNGs"), which are constantly generating random numbers, at a rate of hundreds or perhaps thousands per second. As soon as the "Play" button is pressed, the most recent random number is used to determine the result.

3. **SICS/TICS** – System Internal Controls

4. **SMIB** – Slot Machine Interface Board; a device containing logic and interface boards inside the card box or gaming machine. These boards store machine data until polled by the system

5. TITO – Ticket In Ticket Out; ticketing offered through the use of a validation system as a form of currency exchange at the gaming device

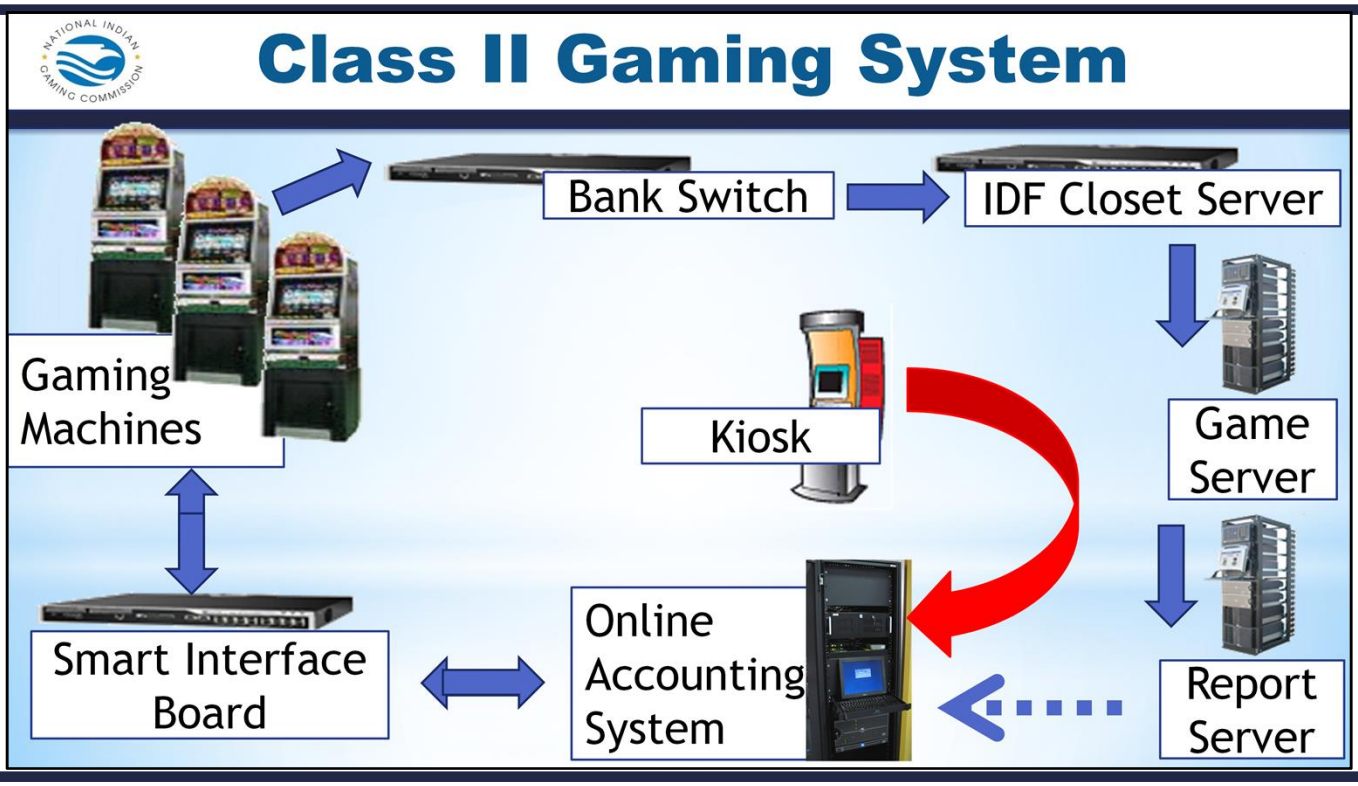
6. MICS – Minimum Internal Controls

7. Paytable - a program that contains the pay amounts as a function of each winning combination and also the virtual reel strips and weightings to arrive at a specified RTP

8. **CMS** - Casino Management System

9. **Remote Access –** Ability to access a computer such as an office network computer from a remote location. This allows individuals to work offsite from another location.

10. **System Verification** – Ability to verify compliant software from a Independent Test Lab with a software verification tool.

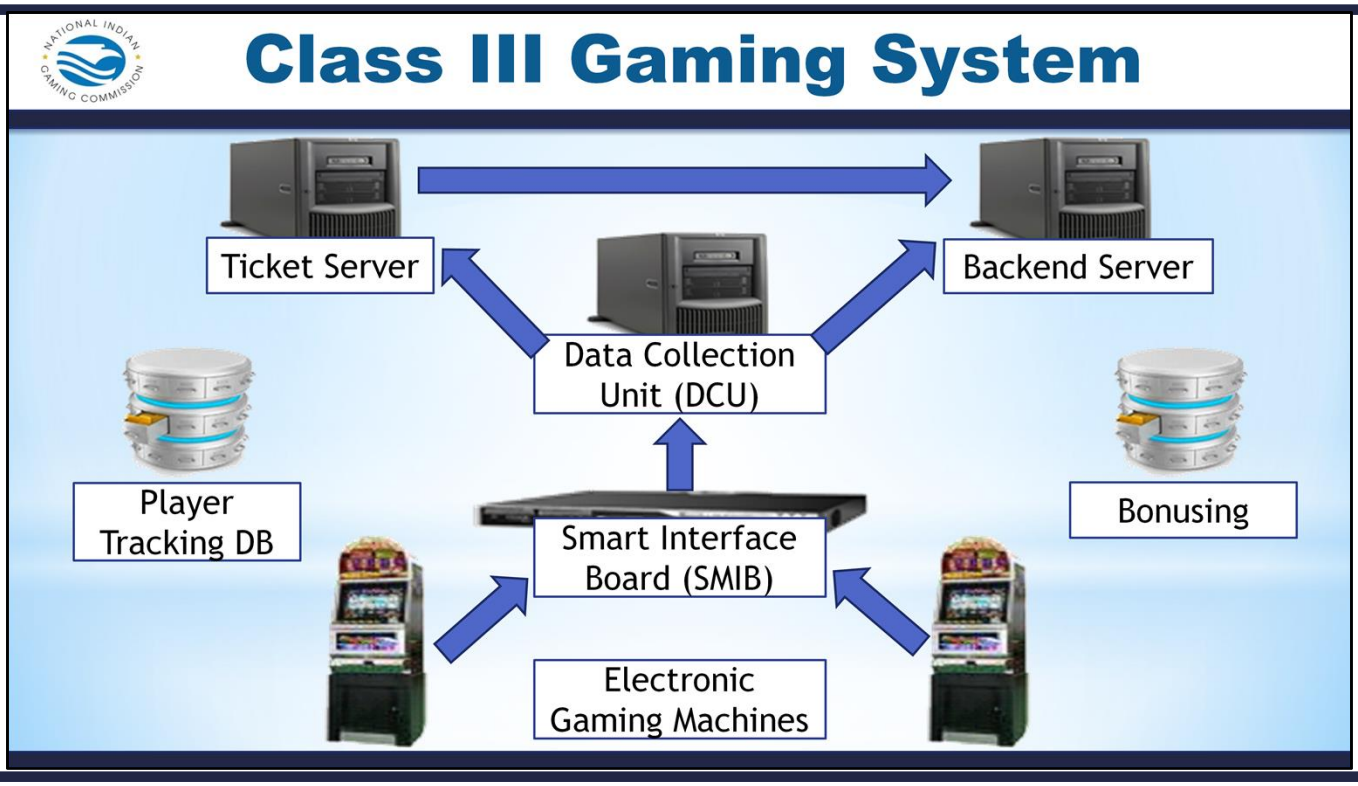


KEY POINTS

1.Player Interface and Bank Switch
2. IDF Closet, Game and Report Server
3. Smart Interface Board, Online Acct. Sys. And Kiosk

IDF closet switch: Intermediate distribution frame is a room (closet) which contains network equipment.

- Smart interface board: gaming device and network interface device adapted to connect a gaming device to a network are provided. The network interface device includes a data handler and a firewall. The data handler has processing and memory resources, and is adapted to perform data handling functions for transferring data between a network and a gaming device controller. The firewall is adapted to inhibit transfer of at least some unauthorized data received from the network to the gaming device controller.



KEY POINTS

- Primary source of game outcomes are determined using reel strip stop positions.
- All logic for the game resides in the cabinet. You are playing against the logic inside the electronic gaming machine.
- There is no minimum player requirement to initiate game play.
- Game play is not contingent upon system connectivity.

Activity #1

In your own words…

KEY POINTS

ACTIVITY – Explaining one of the concepts covered or terminology in your own words.

Group Work

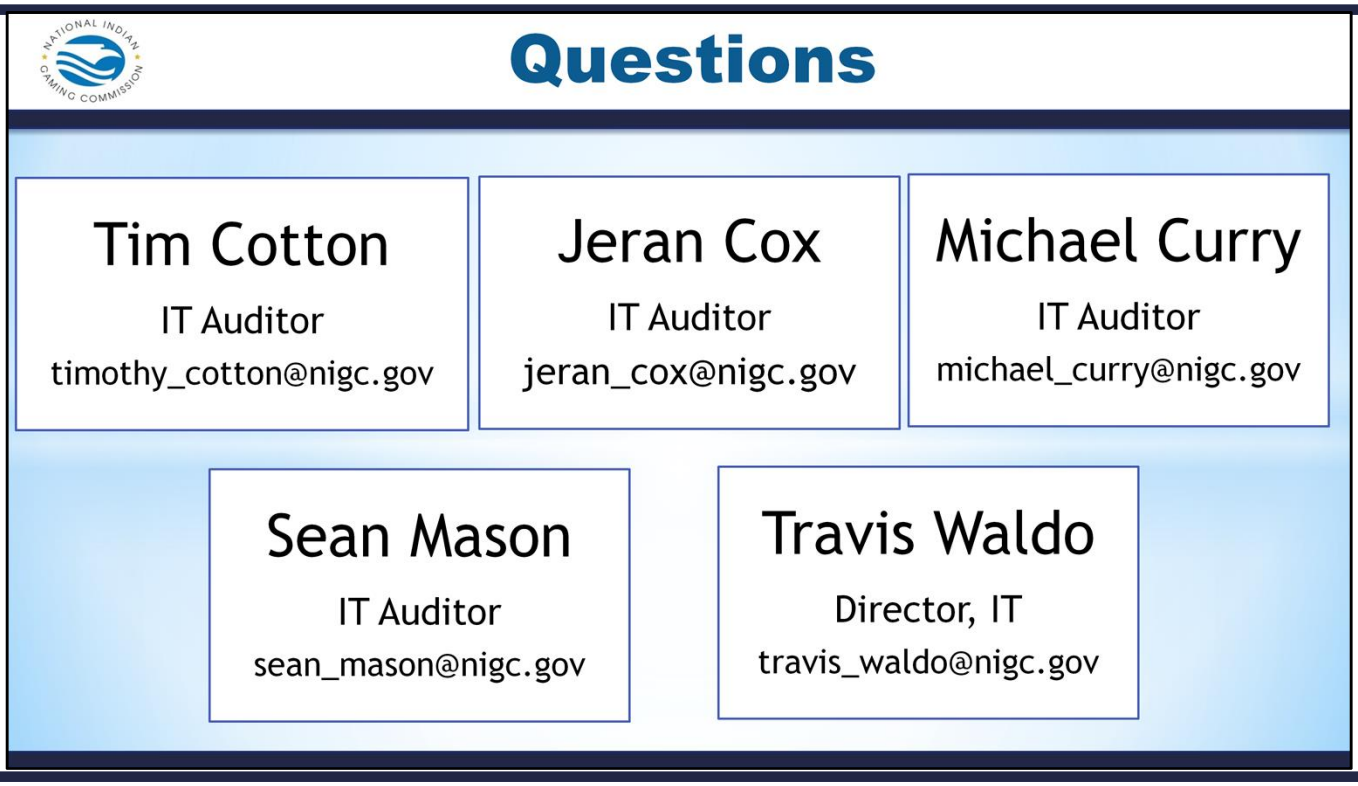
TIME: 15 minutes

Instructions:

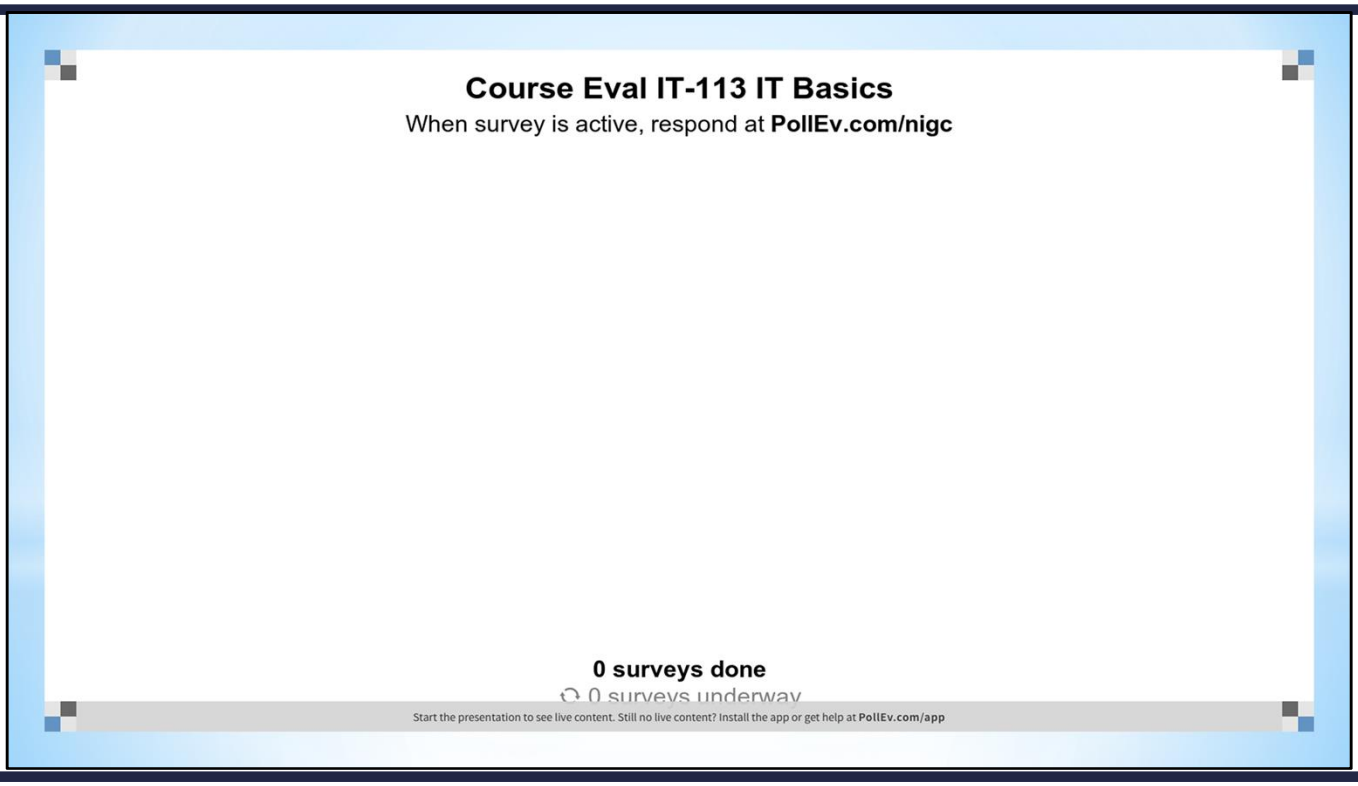
1. Select a note taker and a presenter(the instructor will make assignments)
2. Present your explanation or definition to the class.

KEY POINTS
ACTIVITY – Explaining one of the concepts covered or terminology in your own words.

Group Work
TIME: 15 minutes


Questions
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov
Jeran Cox
IT Auditor
jeran_cox@nigc.gov
Michael Curry
IT Auditor
michael_curry@nigc.gov
Sean Mason
IT Auditor
sean_mason@nigc.gov
Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS



KEY POINTS

Poll Title: Course Eval IT-113 IT Basics

https://www.polleverywhere.com/surveys/9qcpEmUT2

IT-113 IT Basics Glossary

Term	Definition
Action	The total amount of money bet in a specific period of time.
Arm	The gaming machines and/or electronic player interface (slot machine) arm is the lever located traditionally on the right side of the gaming machines and/or electronic player interface (slot machine). This arm/lever is pulled to activate the reels. Also, once pulled the arm stops the RNG and the symbols are determined. In newer gaming machines and/or electronic player interface (slot machine) versus traditional gaming machines and/or electronic player interface (slot machine), the arm no longer actually pulls the reel; they could just as easily use a button to activate the reel.
Bank	This is used in reference to a row of gaming machines and/or electronic player interface (slot machine) in an establishment.
Bars	Bars are a common symbol you'll see on many gaming machines and/or electronic player interface (slot machine). It is usually a rectangular shape with the word BAR printed on it. There are usually single, double, and triple bar symbols on the reel.
Bonus	The bonus on gaming machines and/or electronic player interface (slot machine) refers to a special feature of the particular game theme, which is activated when certain symbols appear in a winning combination. Bonuses vary depending upon the game. Some bonus rounds are a special session of free spins (the number of which is often based on the winning combination that triggers the bonus), often with a different or modified set of winning combinations as the main game, and often with winning credit values increased by a specific multiplier, which is prominently displayed as part of the bonus graphics and/or animation (which in many cases is of a slightly different design or color scheme from the main game). In other bonus rounds, the player is presented with several items on a screen from which to choose. As the player chooses items, a number of credits is revealed and awarded. Some bonuses use a mechanical device, such as a spinning wheel, that works in conjunction with the bonus to display the amount won.
Bonus Game	A secondary event in a gaming machines and/or electronic player interface (slot machine) game that permits the player to win additional money through an activity other than the spinning of reels.
Bonus Multiplier Slots	These machines offer larger top jackpots as incentive for gamers to play max coins. On these machines the top jackpot symbol will only payout if you have played the max coins on that spin.
Bonus Video Slots:	The most graphically loaded glitziest slots to hit the market. These machines offer the chance to go to a second level bonus round. They are known for their many features and options for players.
Call Attendant	When someone hits a major jackpot, this is the person who comes and makes a “hand” payout. Can also refer to the person who oversees the operation of the gaming machines and/or electronic player interface (slot machine).

IT-113 IT Basics Glossary

Term	Definition
Candle	A light on top of the gaming machines and/or electronic player interface (slot machine). It flashes to alert the operator that change is needed, hand pay is requested or a potential problem with the machine.
Carousel	Refers to a grouping of gaming machines and/or electronic player interface (slot machine)s, or many "banks" of gaming machines and/or electronic player interface (slot machine)s. Often times the gaming machines and/or electronic player interface (slot machine) carousels are organized by gaming machines and/or electronic player interface (slot machine)s of a similar type, and the gaming machines and/or electronic player interface (slot machine) grouping traditionally got the nickname "carousel" because the slots are often in an oval or circular shape.
Certified	Certified gaming machines and/or electronic player interface (slot machine) are examined by casino regulators to ensure the gaming machines and/or electronic player interface (slot machine) conforms to the laws for payout percentages. These machines are clearly marked as “certified.”
Class II game characteristics	The player is playing against other players and competing for a common prize. There is not necessarily a winner in each game. The game continues until there is a winner. In a given set there are a certain number of wins and losses. Once a certain combination has occurred it cannot occur again until a new batch is initiated. This is most obvious in scratch-card games using cards that come in packs. Once a card has been pulled from a pack, the combinations on that card cannot occur again until a new pack of cards is installed. One game is dependent on previous games. The player must be an active participant. They must recognize events as they occur and must recognize when they have won and announce their winning. Bingo is an excellent example here. All players play from the same set of numbers as the numbers are announced.
Class III game characteristics	The player is playing against the house. Each game is independent of previous games. Any possible outcome can occur in any game. Wins are announced automatically.
Coin hopper	Normally this is a rotating container (older games) where the coins that are immediately available for payouts are held. The hopper is a mechanical device that rotates coins into the coin tray when a player collects credits/coins (by pressing a "Cash Out" button). When a certain preset coin capacity is reached, a coin diverter automatically redirects, or "drops," excess coins into a "drop bucket" or "drop box." (Unused coin hoppers can still be found even on games that exclusively employ Ticket-In Ticket-Out technology, as a vestige.)
Coin Size	This can reference the size of a bet. On multiple coin gaming machines and/or electronic player interface (slot machine) a player can use more than one coin on a spin.

IT-113 IT Basics Glossary

Term	Definition
Coin-Free Play	Gaming machines and/or electronic player interface (slot machine) play that involves using printed tickets or credit tokens instead of coins.
Coin-In	Refers to the total amount of money a player puts into a gaming machines and/or electronic player interface (slot machine).
Comps	These are complimentary amenities for higher rolling gamblers. Such “comps” may include: free drinks, buffets, show tickets, custom foods, discount hotel rooms, and even cash rebates.
Control (Main) Program	The control program (software that operates the gaming device’s functions such as metering, RNG, control of peripherals, e.g. bill acceptor)
Credit	A credit is the gaming machines and/or electronic player interface (slot machine) equivalent to coins. When you insert coins or bills into the machine you are awarded one credit for each coin. You are also awarded credits for winning spins. Each credit awarded is equivalent to one coin. You can turn your credits back into coins by pressing the Cash Out button on the machine.
Credit meter	A visual LED display of the amount of money or credits on the machine. On video reel machines this is either a simulated LED display, or represented in a different font altogether, based on the design of the game graphics.
Double Machines	These machines pay double or triple if winning combinations of certain symbols line up.
Drop Bucket	Also known as a “drop box,” the drop bucket collects the excess coins that the coin hopper drops. This “bucket” is located at the gaming machines and/or electronic player interface (slot machine)’s base and is collected regularly by the casino. Though the “drop box” and “drop bucket” are similar, traditionally “drop buckets” are found in lower denomination gaming machines and/or electronic player interface (slot machine) whereas “drop boxes” have lids and locks and are used in higher denomination gaming machines and/or electronic player interface (slot machine).
Drop bucket or drop box	A container located in a gaming machines and/or electronic player interface (slot machine)'s base where excess coins are diverted from the hopper. Typically, a drop bucket is used for low denomination gaming machines and/or electronic player interface (slot machine) and a drop box is used for high denomination gaming machines and/or electronic player interface (slot machine). A drop box contains a hinged lid with one or more locks whereas a drop bucket does not contain a lid. The contents of drop buckets and drop boxes are collected and counted by the casino on a scheduled basis.
EGM	Stands for "Electronic Gaming Machine" and is often referred to by initials.

IT-113 IT Basics Glossary

Term	Definition
Flat-Top	"Flat-top" gaming machines and/or electronic player interface (slot machine) pay out a non-progressive jackpot. The name also refers to the gaming machines and/or electronic player interface (slot machine)'s appearance—the machine has a flat-top that allows the player to sit while playing.
Fraud	Mechanical gaming machines and/or electronic player interface (slot machine) and their coin acceptors were sometimes susceptible to cheating devices and other scams. One historical example involved spinning a coin with a short length of plastic wire. The weight and size of the coin would be accepted by the machine and credits would be granted. However, the spin created by the plastic wire would cause the coin to exit through the reject chute into the payout tray. This particular scam has become obsolete due to improvements in newer gaming machines and/or electronic player interface (slot machine). Modern gaming machines and/or electronic player interface (slot machine) are controlled by EPROM computer chips and, in large casinos; coin acceptors have become obsolete in favor of bill acceptors. These machines and their bill acceptors are designed with advanced anti-cheating and anti-counterfeiting measures and are difficult to defraud. Early computerized gaming machines and/or electronic player interface (slot machine) were sometimes defrauded through the use of cheating devices, such as the "slider" or "monkey paw" used by notorious gaming machines and/or electronic player interface (slot machine) cheat.
Hand Pay	Refers to a payout made by an attendant or at an exchange point ("cage"), rather than by the gaming machines and/or electronic player interface (slot machine) itself. A hand pay occurs when the amount of the payout exceeds the maximum amount that was preset by the gaming machines and/or electronic player interface (slot machine) operator. Usually, the maximum amount is set at the level where the operator must begin to deduct taxes. A hand pay could also be necessary as a result of a short pay.
Hard Count	This is the process casinos (and banks) use to count coin currency. The hard count takes place in an extremely secure hard count room and is done through the use of weigh scales. The coins and tokens are divided by denominations, and then placed on a weigh scale programmed to calculate the total amount of the coins. The only exception to using the weigh scales for hard currency is with high end tokens—often $25 dollars or more apiece, these are often hand counted.
Hit	Any winning combination of symbols on the pay line.
Hit Frequency	The frequency/hit rate with which a gaming machines and/or electronic player interface (slot machine) registers a winning combination relative to the number of games played.

IT-113 IT Basics Glossary

Term	Definition
Hold and Re-spin	A non-traditional style gaming machines and/or electronic player interface (slot machine) that allows a player to hold one or more of the gaming machines and/or electronic player interface (slot machine) reels and spin the rest of the reels again. This type of gaming machines and/or electronic player interface (slot machine) gives the player the chance to obtain a better combination of reels on the second spin.
Hold Percentage	The “hold” is discussed among casino executives. It is the opposite of the payback percentage, and represents the amount of money the casino is making from a machine or the slot department in general. This can be thought of as a betting fee.
Hopper	This is where the money is stored inside the machine. When the hopper overflows, the excess change flows over into a bucket. The "excess" is the profit the casino takes home. Hoppers are generally emptied in the morning before the crowds arrive.
House	Another term for casino. Casino literally translates as house in Italian.
House Edge	Also known as Hold. Expressed as a percentage, this is the amount of money the casino holds out of a bet as profit for the casino. This can be thought of as a betting fee. It is the opposite of the payback percentage, and represents the amount of money the casino is making from a machine or the slot department in general.
Jackpot	A gaming machines and/or electronic player interface (slot machine)’s highest payout or can references the top prize in any gambling game.
Linked machines	Often machines are linked together in a way that allows a group of machines to offer a particularly large prize, or "jackpot." Each gaming machines and/or electronic player interface (slot machine) in the group contributes a small amount to this progressive jackpot, awarded to a player who gets, for example, a royal flush on a video poker machine or a specific combination of symbols on a regular or nine-line gaming machines and/or electronic player interface (slot machine). The amount paid for the progressive jackpot is usually far higher than any single gaming machines and/or electronic player interface (slot machine) could pay on its own.
Load	Used as a verb. To play the maximum number of coins or tokens allowable in a specific gaming machines and/or electronic player interface (slot machine).
Loose Machine	A gaming machines and/or electronic player interface (slot machine) that is paying out well. This is likely because it is set with a higher payout percentage.
Low Level	Also known as a “Slant Top” gaming machines and/or electronic player interface (slot machine), this type of slot includes a stool so that players can sit while they play.
Max Bet	The maximum amount a player can bet on one spin.

IT-113 IT Basics Glossary

Term	Definition
MEAL book (Machine entry authorization log)	A log of the employee's entries into the machine.
Mechanical Slots	This refers to the traditional gaming machines and/or electronic player interface (slot machine) that operate with mechanical reels.
MODIFY (AP)	A status used to classify a product that has been modified from its' previous version, which may include: 1. Manufacturer name change; 2. Future implementation of new technology; 3. Additional support for new peripheral equipment (Bill Validator, Printer).
Multiline /Multi-line	A gaming machines and/or electronic player interface (slot machine) with more than one pay line. Gaming machines and/or electronic player interface (slot machine) may have several pay lines.
Multiplier	A gaming machines and/or electronic player interface (slot machine) with a pay schedule where the pay schedule for each winning combination is multiplied evenly by each coin wagered.
NON-MANDATORY UPGRADE (NU)	A status used to classify a product that has been superseded by a non-critical upgraded version. Items classified as obsolete may remain in use but it is recommended NU items not be used for new installations. An 'NU' status generally indicates that the software still fully meets the applicable technical standards of the jurisdiction. Reasons for this assigned status may include: 1. Inconsequential bug fixes which do not constitute a revocation; 2. Program enhancements in the form of new features; 3. Help screen verbiage clarification which does not constitute a revocation; 4. Issues that require a power cycle to restore (inconvenient but not critical).
Not Approved (NA)	Status for items that have not been tested against or meets GLI-11 standards for Gaming devices in Casinos and/or under the GLI-13 standards for On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos.
Odds	The probability of an event. Odds are traditionally expressed as a ratio.
Optimal Play	This is the payout percentage if a player uses the optimal strategy on a skill based gaming machines and/or electronic player interface (slot machine).
Pay Cycle	This refers to a belief among slots players that a machine might be due to payout in order to meet the payout percentage. It is important to understand that the payout percentages work over the course of thousands of plays.

IT-113 IT Basics Glossary

Term	Definition
Pay For Play	These are generally one-two-three coins option gaming machines and/or electronic player interface (slot machine) with staggered payoffs. The more coins you put the better the payoffs.
Pay Line	Usually the line in the middle of the slot window but also it can be three lines, five lines or even more on video slots. Only symbols on a pay line will result in a win.
Pay Table	This is the payoff schedule. It tells you what symbols you need to line up to win and how much you will be paid if you get the right order. Many gaming machines and/or electronic player interface (slot machine) have the pay table printed directly on the machine. However, most video gaming machines and/or electronic player interface (slot machine) have opted to hide the pay table. For these, you simply need to hit a button to bring it up. Online slots usually have the pay table posted on the same screen or via a button on the machine.
Payback	The percentage of winnings a machine will payout in relation to the amount put in, also known as payout percentage.
Payback Percentage	This is the amount of money the gaming machines and/or electronic player interface (slot machine) eventually pays back to its slot players. This number is not over a few spins, but rather, covers tens or even hundreds of thousands of spins. This term is often misunderstood. The payback percentage applies to total dollars run through the machine and not the money you personally have entered.
Pay-line:	The pay-line is the line drawn on the glass or screen where the symbols must line up to create a payoff. Many newer gaming machines and/or electronic player interface (slot machine), especially video gaming machines and/or electronic player interface (slot machine) have many V-shaped pay-lines that go up, down, across, and diagonally.
Personality (Data) Program	The personality program (software that contains data example reel strips, cards, help screens, graphic sequences to be used by main program)
Poker Machine	Also known as “pokie.” The name for a gaming machines and/or electronic player interface (slot machine) in Australia.
Progressive Jackpot	The jackpot on a gaming machines and/or electronic player interface (slot machine) grows as each bet is played. There are two types of progressive jackpots: individual progressive jackpot and multiple progressive jackpot. Individual jackpot is a progressive jackpot that only builds on the bets of one gaming machines and/or electronic player interface (slot machine). Multiple jackpots build as bets are placed on multiple gaming machines and/or electronic player interface (slot machine). More than one gaming machines and/or electronic player interface (slot machine) is linked to a single progressive jackpot; jackpots grow very quickly on multiple progressive jackpots.

IT-113 IT Basics Glossary

Term	Definition
Progressive Slots	A group of gaming machines and/or electronic player interface (slot machine) linked together to pay one common big jackpot.
Progressive Ticker	Also known as a Progressive Meter. This shows how much a progressive jackpot is worth.
Random Number Generators	All modern machines are designed using pseudo random number generators ("PRNGs"), which are constantly generating random numbers, at a rate of hundreds or perhaps thousands per second. As soon as the "Play" button is pressed, the most recent random number is used to determine the result. This means that the result varies depending on exactly when the game is played.
Reels	The symbol-covered wheel. In traditional gaming machines and/or electronic player interface (slot machine), these reels spin around and come to a stop in random fashion dictated by the payout percentage. There are multiple types of reel games i.e. three, four and five reels to name a few. The more reels the harder it is to hit a jackpot.
REVOKED (RV)	A status used to classify items that should be removed from use due to the Existence of critical issues. A jurisdiction has the choice of continuing to use items that have been placed in a revoked status. A 'RV' status generally indicates that the software does not meet the applicable technical standards of the jurisdiction; however, please be reminded, revocations may also at times be requested by the gaming suppliers due to compatibility issues that are unrelated to compliance with the technical standards. Reasons for revocation may include: 1. Game integrity issues; 2. Affects accounting/revenue reporting; 3. Issues which may prompt a patron dispute; 4. Previous version was found to be non-compliant with jurisdictional regulation; 5. Malfunctions requiring a RAM Clear; 6. Help/Pay screen was incorrect or misleading; 7. Loss of data.
RNG	Each gaming machines and/or electronic player interface (slot machine) has a computer chip in it that selects random numbers. RNG means Random Number Generator. The RNG determines if your spin is a winner or loser. This computer chip constantly cycles though numbers until a coin is placed in the gaming machines and/or electronic player interface (slot machine). Once the button or lever is pushed the reel stops on the symbol combination determined by the number the RNG stopped on as the coin was inserted.
Rollup	The sounds used to announce a win while the gaming machines and/or electronic player interface (slot machine) meters tally the amount won.

IT-113 IT Basics Glossary

Term	Definition
Scatter Pay	Scatter pay gaming machines and/or electronic player interface (slot machine) are ones that will pay you something back just for having a particular symbol anywhere in the window. Rather than paying out based on winning symbols aligning on a single payline, scatter pay gaming machines and/or electronic player interface (slot machine) allow the winning combinations to be “scattered” across the screen.
Short Pay	References a gaming machines and/or electronic player interface (slot machine) partial payout of a players gaming machines and/or electronic player interface (slot machine) winnings. If the coin hopper is low, a gaming machine and/or electronic player interface (slot machine) attendant or the cage will hand pay the remainder amount due to the player.
Signature Slots	The house brand of gaming machines and/or electronic player interface (slot machine). Casinos create their own brand of looser gaming machines and/or electronic player interface (slot machine) to generate PR for the casino.
Slant Top Slot	Also known as a “Low Level” gaming machines and/or electronic player interface (slot machine), this type of slot includes a stool so that players can sit while they play.
Slot Club	A frequent gaming machines and/or electronic player interface (slot machine) player can join a slot club at a casino to earn rewards and incentives for time and money spent at the gaming machines and/or electronic player interface (slot machine). A player receives a slot club card which is then inserted into a gaming machines and/or electronic player interface (slot machine) while a player is gaming. The card then records the time and money spent on the slots and rewards bonuses and comps accordingly.
Slot Placement	Strategy facilities use to tempt players; facilities generally position the better paying gaming machines and/or electronic player interface (slot machine) in areas where other players can see gaming machines and/or electronic player interface (slot machine) payout.
Slot Schedule	This is information posted on the front of slot that discloses what type of slot, denomination, and win amounts possible for each coin played.
Slot Talk	The information traded between players, a good way to improve slots knowledge.
Slot Tournament	A special event in which players compete for preset cash prizes on specially programmed gaming machines and/or electronic player interface (slot machine), receiving points for accumulated credits. Tournaments are free for players and during a tournament a player doesn’t use coins to activate the machines. Tournament prizes are based off the number of credits a player accumulates during the competition. Often times the freebies and prizes are worth significantly more than the price of admission into the tournament.

IT-113 IT Basics Glossary

Term	Definition
Slots	The nickname for gaming machines and/or electronic player interface (slot machine).
Slots Drop	The amount of money that goes through the gaming machines and/or electronic player interface (slot machine).
Stand Up Slot	Also known as an “Upright” gaming machines and/or electronic player interface (slot machine), this type of machine allows player to stand up while playing.
Stops	This is the dead space between the symbols on a reel. When a reel spins around and a symbol does not land on a payline, it has landed on a stop.
Symbols	These are the fun characters and items that appear on the gaming machines and/or electronic player interface (slot machine)'s reel. A common symbol is a colored bar or a piece of fruit, like a cherry.
Take/Pay Cycle	Based on the assumption that most gaming machines and/or electronic player interface (slot machine) work on cycles, it is when to expect a machine to pay out following a certain amount of money fed into the game.
Theoretical Hold Worksheet	A document provided by the manufacturer for all gaming machines and/or electronic player interface (slot machine), which indicates the theoretical percentage that the gaming machines and/or electronic player interface (slot machine) should hold based on the amount paid in. The worksheet also indicates the reel strip settings, number of coins that may be played, the payout schedule, the number of reels and other information descriptive of the particular type of gaming machines and/or electronic player interface (slot machine).
Tight Machine	A gaming machines and/or electronic player interface (slot machine) that is not paying much out. This is likely because it is set with a lower payout percentage.
Tilt	This term originates with the older mechanical gaming machines and/or electronic player interface (slot machine). Mechanical gaming machines and/or electronic player interface (slot machine) had tilt switches. If a coin is jammed in the gaming machines and/or electronic player interface (slot machine) now, the tilt light comes on, if the machine owes the player any winnings it is stored in the memory and pays out once the problem is fixed. Today, the term tilt can refer to many different kinds of mechanical failure from reel motor failure to door switch problems.
Token	A form or payment gaming machines and/or electronic player interface (slot machine) take to authorize a play. The tokens work just like coins and can be bought to represent different monetary denominations.
Upright	Also known as a “Stand Up” gaming machines and/or electronic player interface (slot machine), this type of machine allows player to stand up while playing.

IT-113 IT Basics Glossary

Term	Definition
Video Lottery Terminal	Video lottery terminal is connected to a centralized computer system that allows the lottery jurisdiction to monitor game play and perform control functions. A video lottery terminal at a minimum will utilize randomness in determination of prizes, contain some form of activation to initiate the selection process, and make use of a methodology for delivery of the determined outcome.
Video Gaming machines and/or electronic player interface (slot machine)	A gaming machines and/or electronic player interface (slot machine) with a video screen on which the reels and other elements are simulated with graphics and animation.
Virtual Reel	Virtual reels are on video gaming machines and/or electronic player interface (slot machine) and they rely on computerized selection of reel symbols. Just like mechanical reels, the results are determined by the RNG.
Volatility	The ratio of size versus frequency of jackpots in a slot game.
Wild Symbol	Essentially acts like the joker in some cards came. The wild symbol can act as any other symbol on the reel.

IT-113 IT Basics Glossary

Table of Acronyms/Abbreviations Networking

ARP	Address Resolution Protocol
ATA	Advanced Technology Attachment
C&A	Certification and Accreditation
CCE	Common Configuration Enumeration
CGE	Cisco Global Exploiter
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FrSIRT	French Security Incident Response Team
FTP	File Transfer Protocol
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GUI	Graphical User Interface
HHS	Department of Health and Human Services

IT-113 IT Basics Glossary

HTTP	Hypertext Transfer Protocol
IAM	Information Assessment Methodology
ICMP	Internet Control Message Protocol
IDART	Information Design Assurance Red Team
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Server
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Standards Organization
ISSO	Information Systems Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
IV	Initialization Vector
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NIS	Network Information System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OS	Operating System
OSSTMM	Open Source Security Testing Methodology Manual

IT-113 IT Basics Glossary

OWASP	Open Web Application Security Project
P2P	Peer-to-Peer
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
POA&M	Plan of Action and Milestones
POP	Post Office Protocol
RF	Radio Frequency
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSN	Social Security Number
STD	Security Tool Distribution
TCP	Transmission Control Protocol

IT-113 IT Basics Glossary

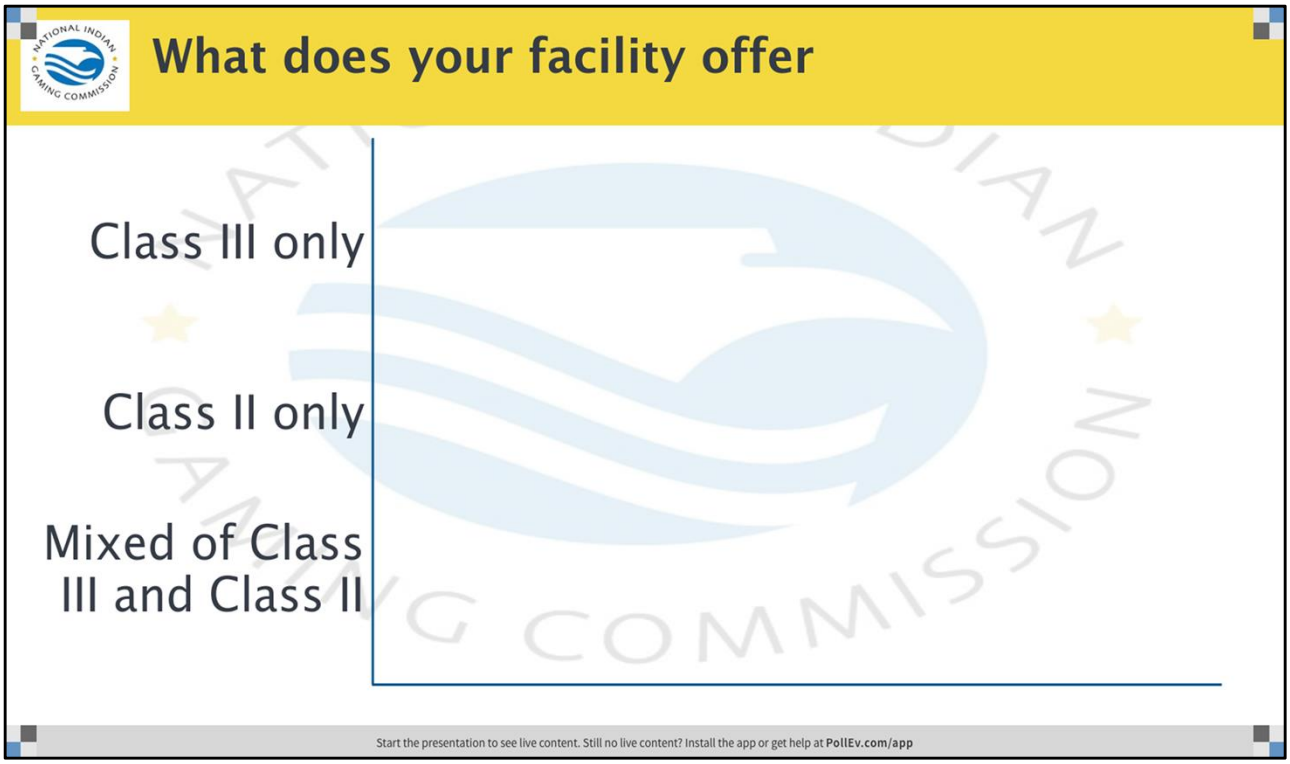
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TFTP	Trivial File Transfer Protocol
THC	The Hacker's Choice
UDP	User Datagram Protocol
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIDPS	Wireless Intrusion Detection and Prevention System
WLAN	Wireless Local Area Network
WVE	Wireless Vulnerabilities and Exploits
XML	Extensible Markup Language

IT-110 Refining & Enhancing IT TICS

IT-110 Refining & Enhancing IT TICS

Information Technology Division

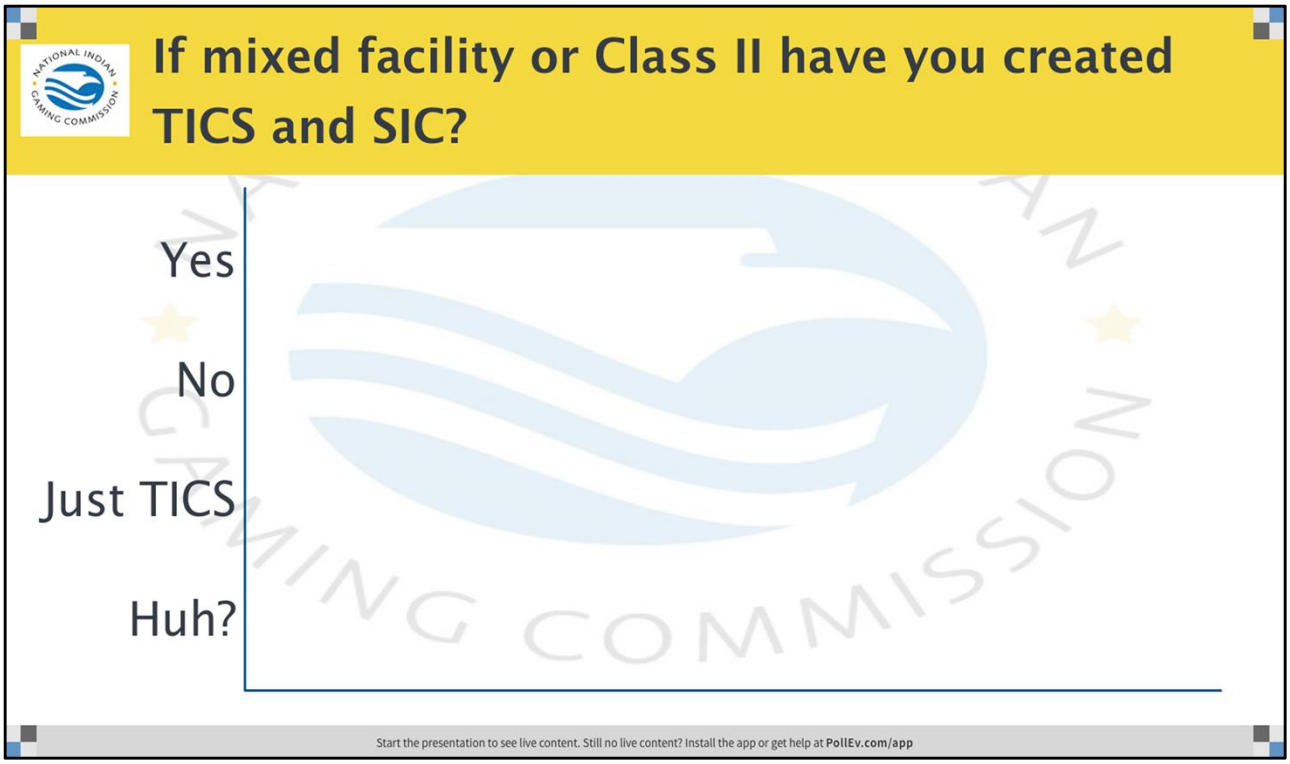
KEY POINTS



KEY POINTS

Poll Title: What does your facility offer

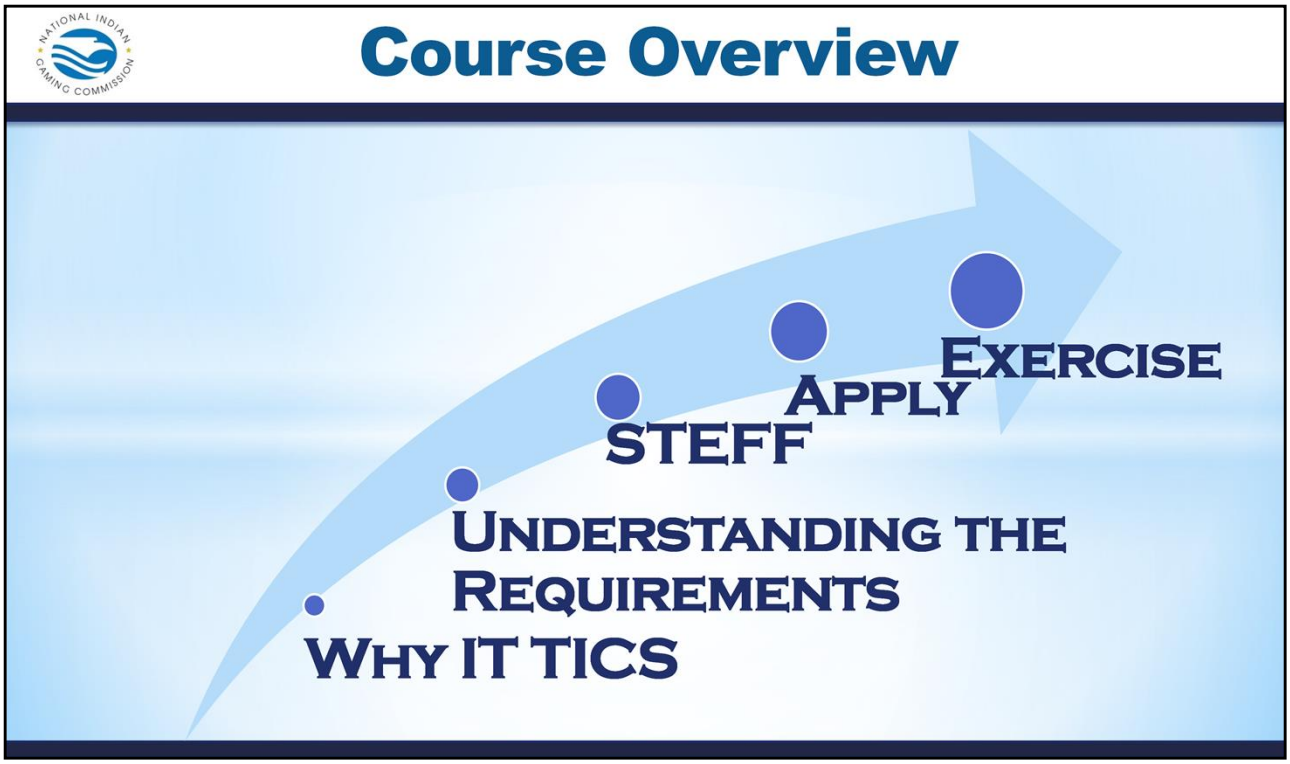
https://www.polleverywhere.com/multiple_choice_polls/NNFvAQgmzJeMpBw



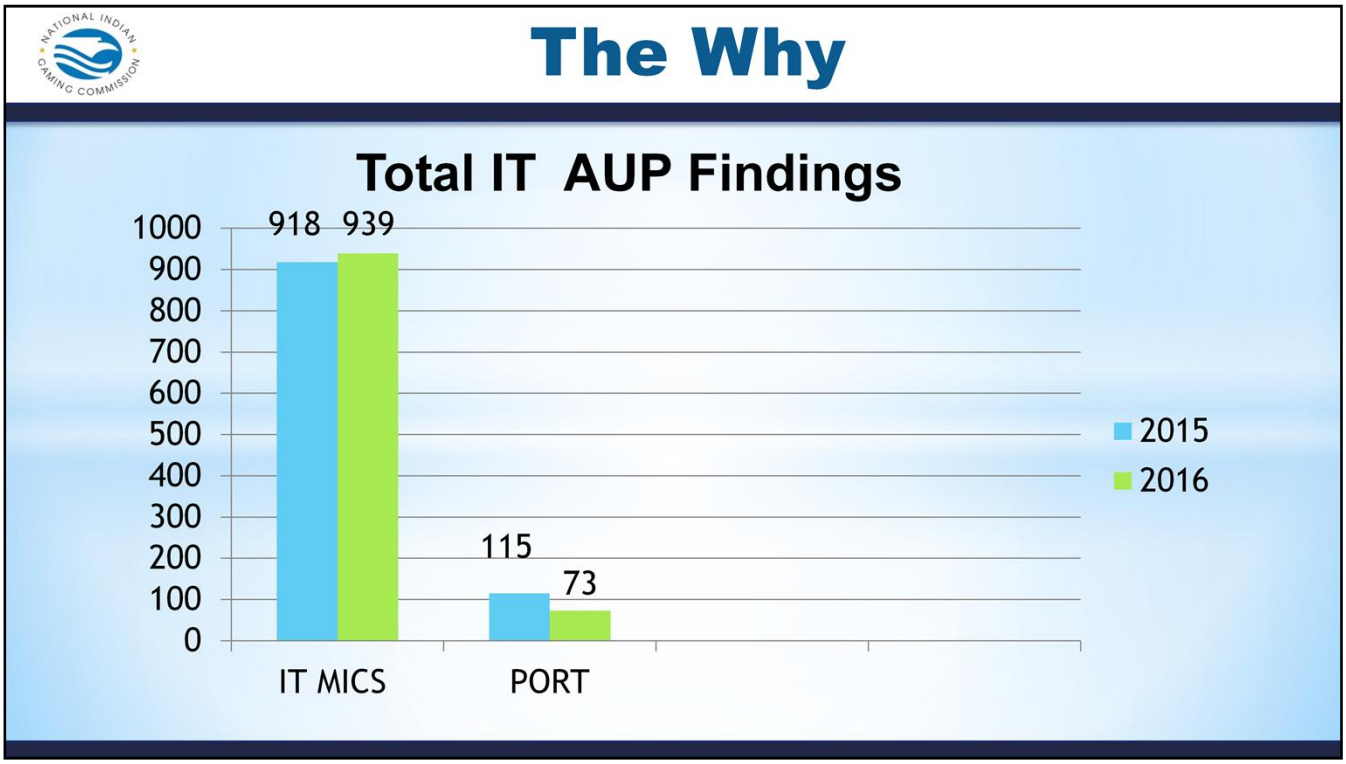
KEY POINTS

Poll Title: If mixed facility or Class II have you created TICS and SIC?

https://www.polleverywhere.com/multiple_choice_polls/GFJu2NGRQGmiFl3


Course Overview
Why IT TICS
Understanding the Requirements
STEFF
Apply
Exercise

KEY POINTS



KEY POINTS

Comparing years 2015 & 2016 for IT Findings.

Enhancing IT TICS are based on the findings from Compliance Audits from all 7 NIGC regions and in this case your individual region.

Common Findings

- Of the 6245 total AUP findings IT accounts for 15% of all the MICS.
- 543.20(i)(2) is the most common finding

KEY POINTS

Overview of Agreed Upon Procedures (AUP) and the importance of reducing critical IT Findings for operations

543.20(i)(2)

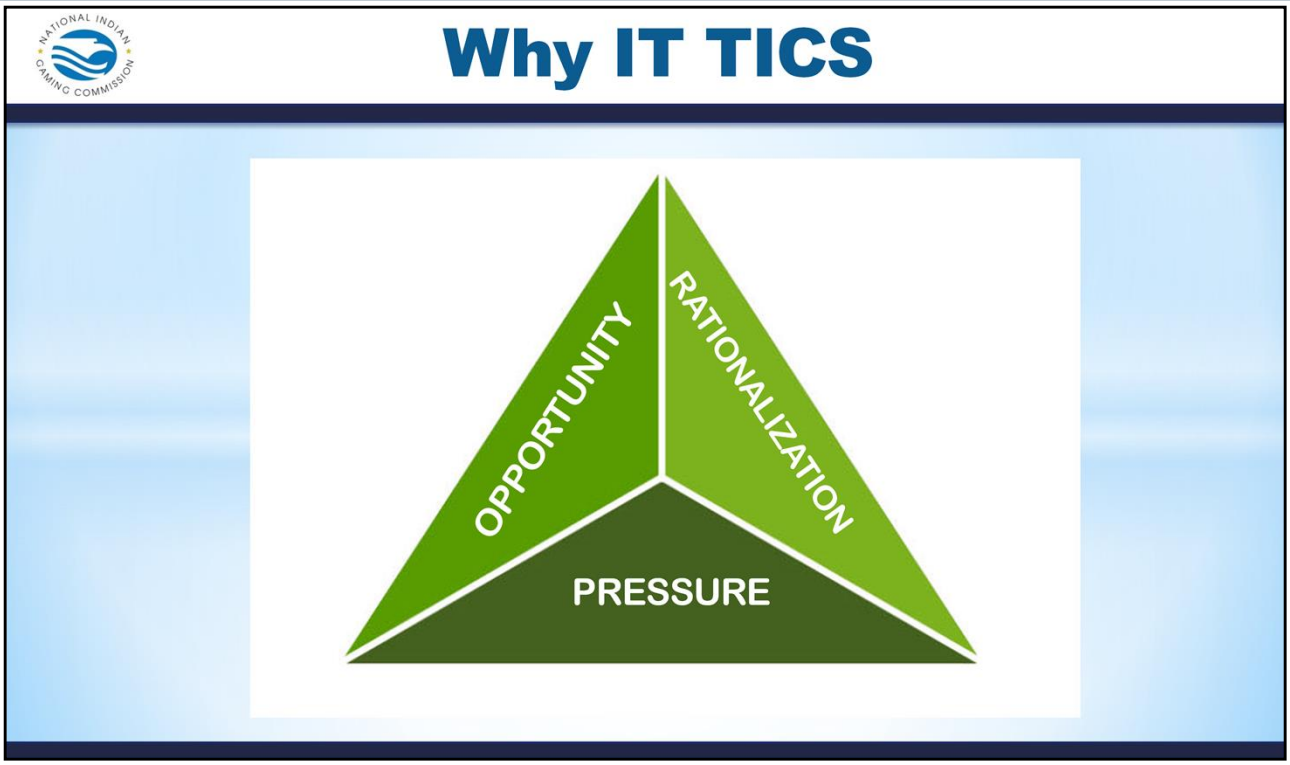
(i) ***Incident monitoring and reporting.***

(1) Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

(2) All security incidents must be responded to within an established time period approved by the TGRA and formally documented.

KEY POINTS

543.20(i)(2) is the most common IT finding by all 7 regions. This finding is around the lack of procedures implemented during the TICS/SICS process by operations.



KEY POINTS

- Internal controls provide reasonable assurances for asset protection, risk mitigation, and reduction in opportunities.
- Pressure - Motivation can be personal financial pressure such as debt problems and/or workplace debt to steal from the operations. i.e. gambling debt or maintaining a certain lifestyle
- Opportunity – An clear case of abuse of their position to solve their financial problems.
- Rationalization - A means of how an individual can/will defraud the operation. Many criminals are first time fraudsters and don't see themselves as criminals but rather a victim of circumstance. i.e. taking care of family or a dishonest employer

MICS - §543.20

What are the minimum internal control standards for information technology and information technology data?

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate…

KEY POINTS

Looking at Section C of 543.20 what does this one standard mean?

Is this standard enough to ensure proper coverage of your operations.

KEY POINTS

Importance of TICS and implementing SICS the procedures associated to internal TICS

MICS §543.20

(c) Class II gaming systems' logical and physical controls.

(1) Control of physical and logical access to the information technology environment,

(2) Physical and logical protection of storage media and its contents

(3) Access credential control methods

(4) Record keeping and audit processes

(5) Departmental independence

KEY POINTS

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems,

among others used in conjunction with Class II gaming;

(2) Physical and logical protection of storage media and its contents, including recovery procedures;

(3) Access credential control methods;

(4) Record keeping and audit processes; and

(5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments

Exercise #1 – Handout #1

1. Review Exercise #1 Handout #1
2. Answer these questions:

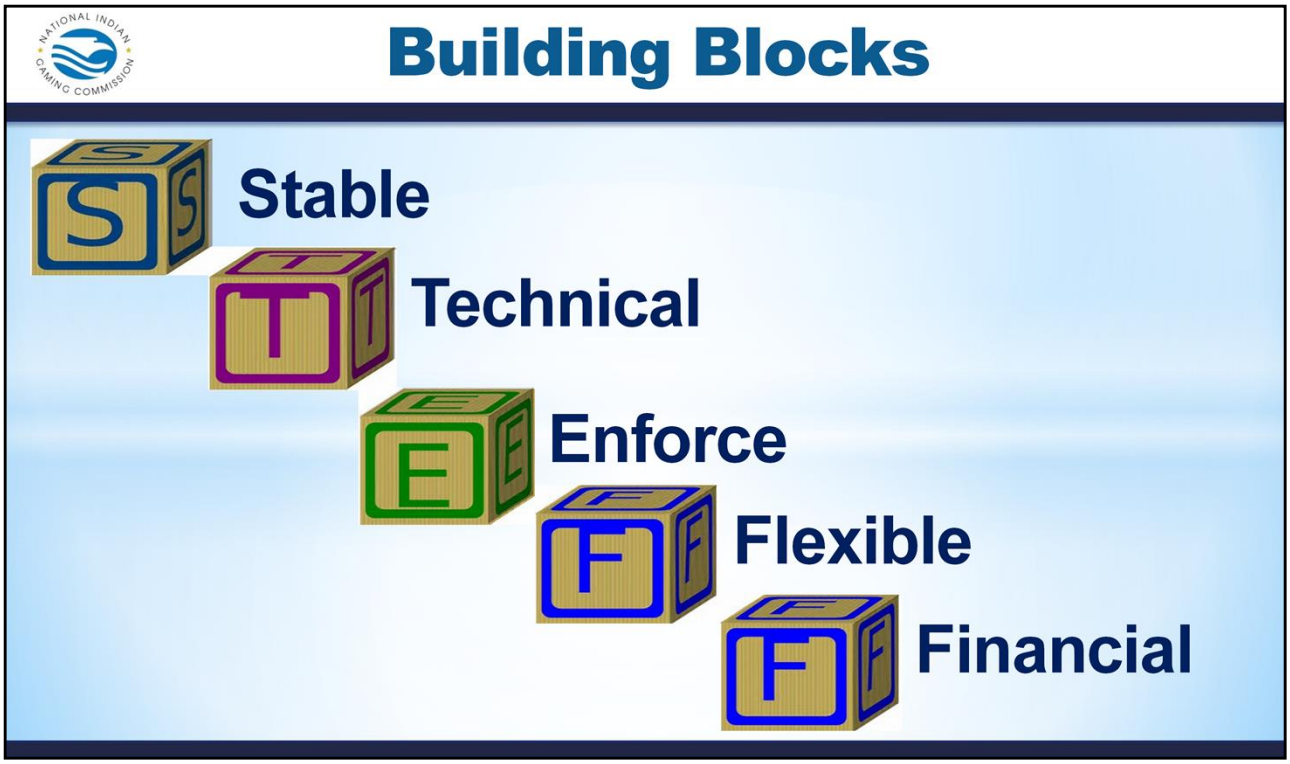
Should the TGRA expand on this Control ?
Why or Why Not?

KEY POINTS
Activity: Discussion - Expanding Controls
TIME: 5 minutes

Instructions:
1. Working at your tables, review this control:
§543.20
(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:
(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

2. Discuss and answer these questions:

Should the TGRA expand on this Control?
-and-
Why or Why Not?



KEY POINTS

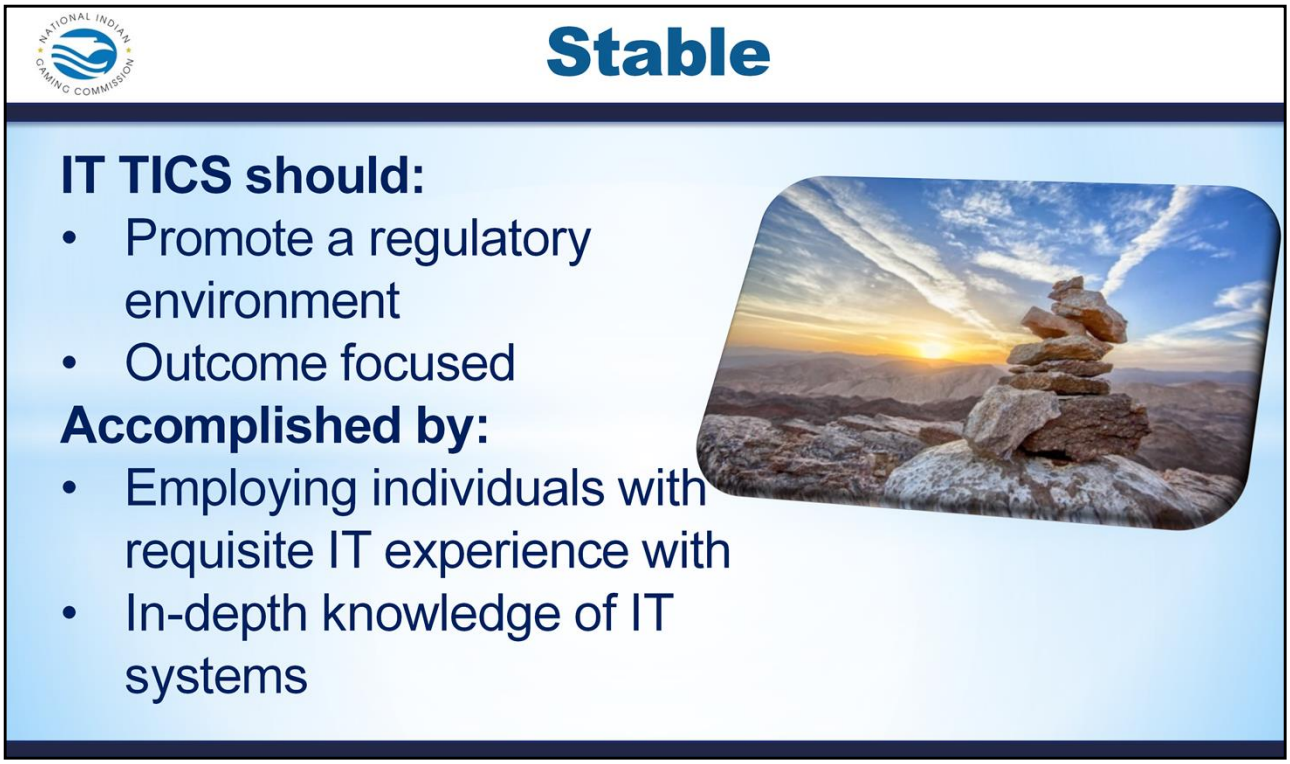
Stable – Firm, Established, Secure, Solid, Steady

Technical – Practical, Scientific, High-tech, maybe mechanical (according to a strict application or interpretation of the rules)

Enforce – Impose, Apply, Administer, Implement, mandatory, binding, contractual

Flexible – pliable, stretch, springy, adaptable, adjustable, versatile, variable, open-ended, cooperative

Financial – Economic impact, fiscal, banking, investment



KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Stability the initial building block for STEFF should provide a foundation for creating your TICS/SICS.

KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

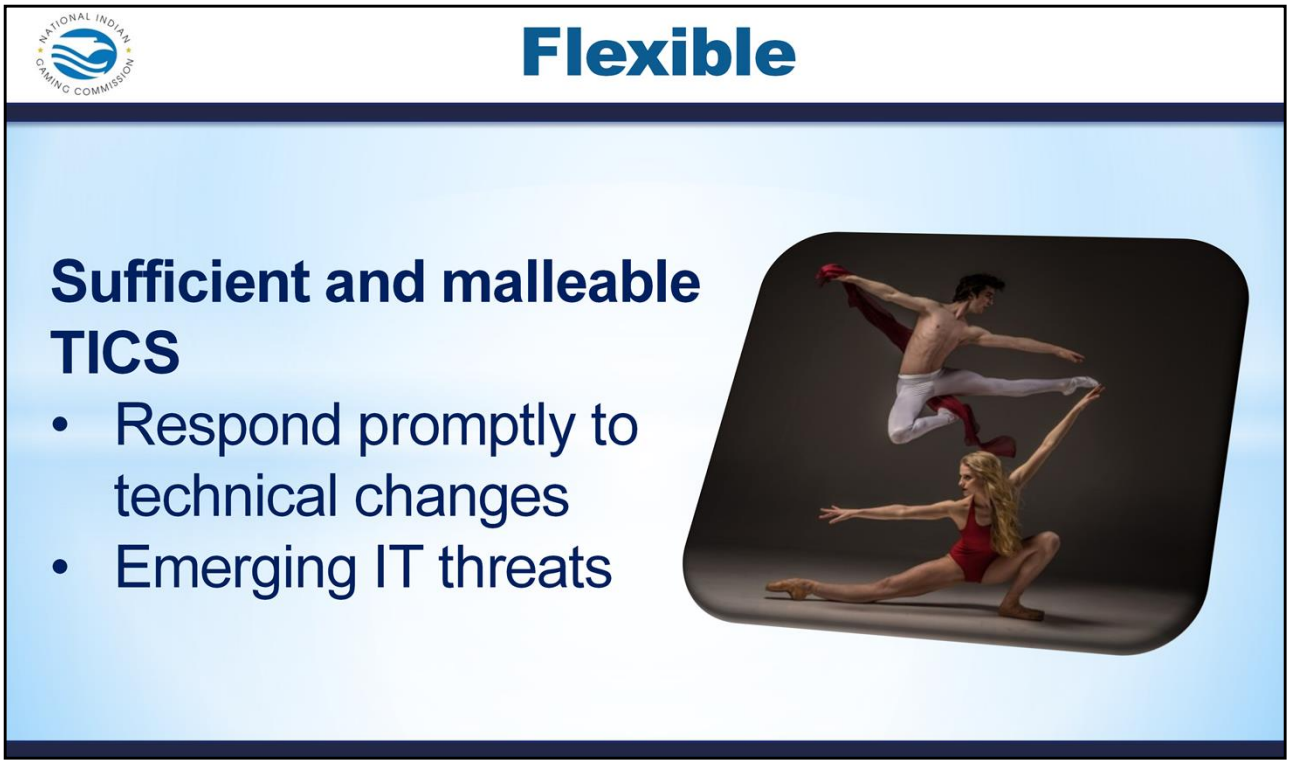
Technical the second foundational principle of STEFF is important to ensure your team has reviewed and included all pertinent technical aspects to your TICS/SICS.

KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Enforcement the third principle in the STEFF model should include the ability to execute and/or enforce the TICS/SICS within your operations.



KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Flexible the fourth principle in STEF infers that all of your TICS/SICS should have enough movement to change with the IT world without having to change them all of the time.

Financial

TICS should

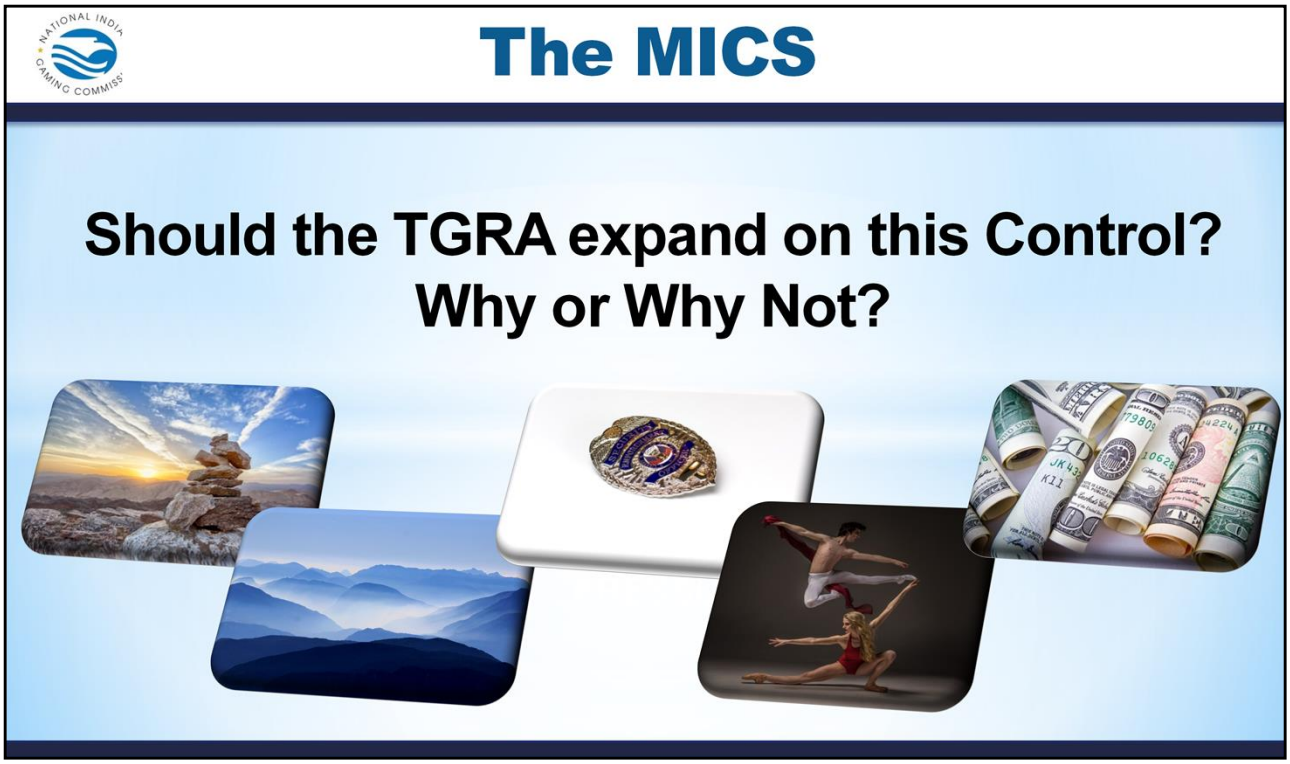
- Be cost-effective
- Not encumber your IT team
- Protect assets with resilient IT TICS

KEY POINTS

Because most Tribal operations adopt the minimum internal compliance standards (MICS) as their TICS it would be better to review and add some depth to your TICS/SICS.

Each building block in the STEFF model is intended for your operations to review your TICS/SICS and ensure they are comprehensive enough to adjust to the ever changing Information Technology Environment.

Financial the fifth and final principle of STEFF should always play an important role in the building blocks in either cost effectiveness of hardware/software required as well as not be constricted in applying the pertinent IT components.



KEY POINTS

See 543.20(c) 1-5

MICS §543.20

(c) Class II gaming systems' logical and physical controls.

(1) Control of physical and logical access to the information technology environment,

(2) Physical and logical protection of storage media and its contents

(3) Access credential control methods

(4) Record keeping and audit processes

(5) Departmental independence

KEY POINTS

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems,

among others used in conjunction with Class II gaming;

(2) Physical and logical protection of storage media and its contents, including recovery procedures;

(3) Access credential control methods;

(4) Record keeping and audit processes; and

(5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments

Exercise #2 – Handout #1

1.Review Exercise #1 Handout #1.

2. Write additional controls for this standard.

KEY POINTS
Activity: Discussion - Expanding Controls
TIME: 20 minutes
Instructions
1. Choose a note taker and presenter.
2. Working at your tables, review this control:

§543.20
(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:
(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

Applying Knowledge

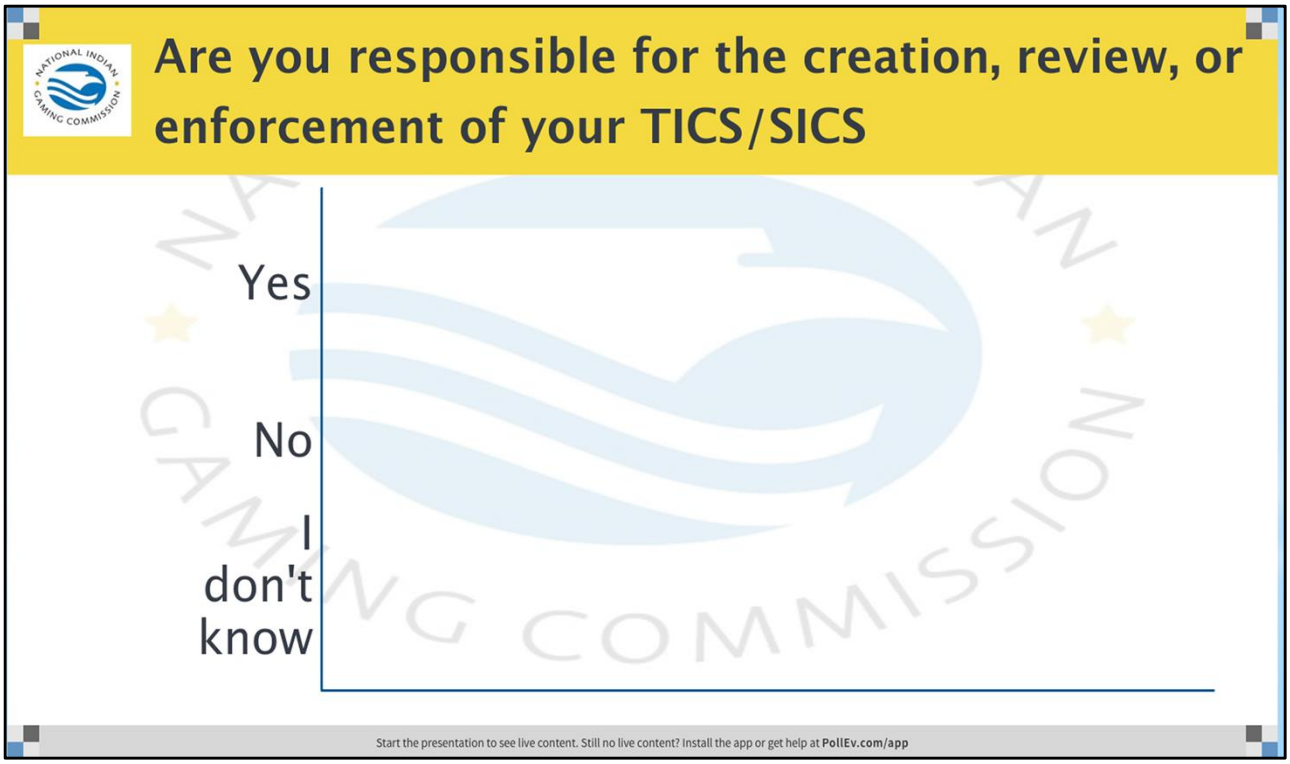
TIC 1 with STEFF

All aspects of a wireless network, including all hardware and software used therein, shall be subject to testing by the commission or an approved independent testing laboratory designated by the commission, and review and approval by the commission prior to the sale, installation, or use of the network by a licensed organization. The cost for which in all cases shall be borne by the licensed manufacturer.

22

KEY POINT

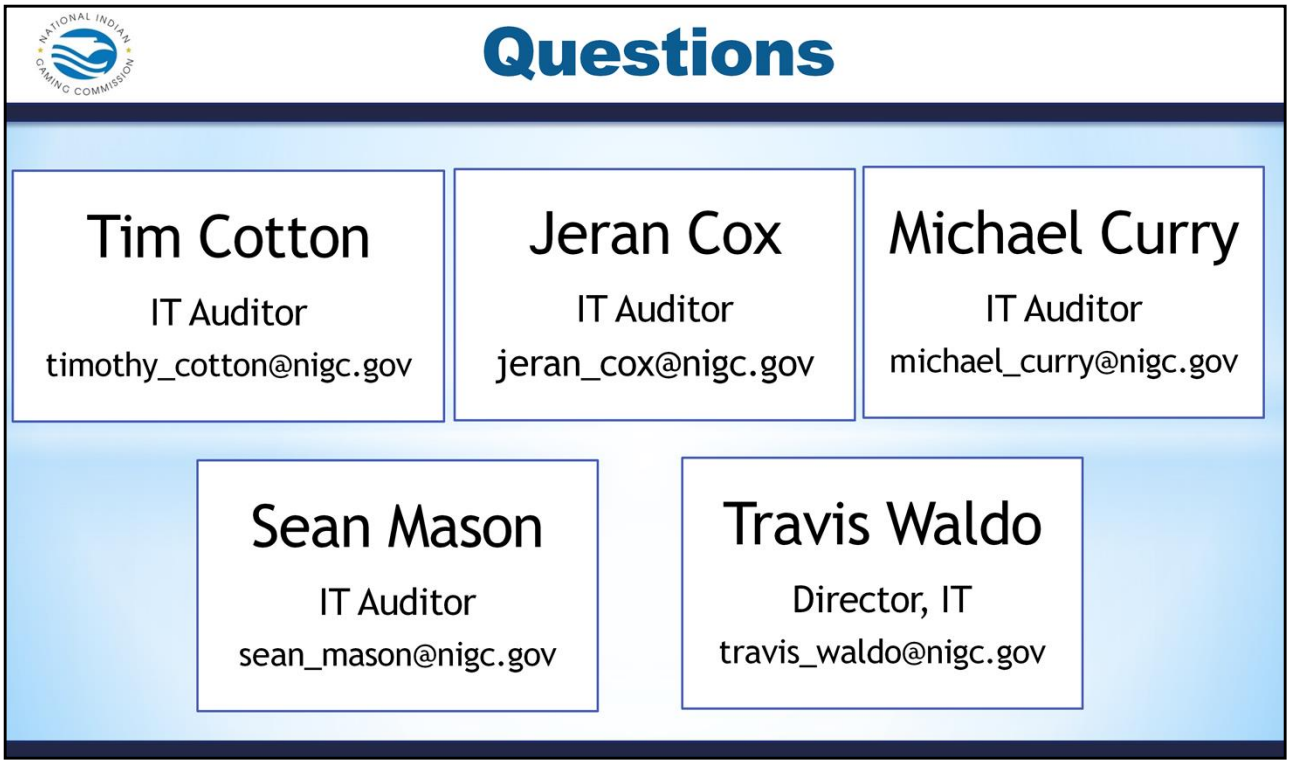
A TIC/SIC that demonstrates the STEFF principle



KEY POINTS

Poll Title: Are you responsible for the creation, review, or enforcement of your TICS/SICS

https://www.polleverywhere.com/multiple_choice_polls/CEjhhc4JyBOPAax


Questions
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov
Jeran Cox
IT Auditor
jeran_cox@nigc.gov
Michael Curry
IT Auditor
michael_curry@nigc.gov
Sean Mason
IT Auditor
sean_mason@nigc.gov
Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS


Course Evaluation
• Provide an honest assessment of your experience
• Written suggestions and comments are greatly appreciate and allow us to improve your experience

KEY POINTS

IT-110 Exercise #1 Handout #1

Instructions

1. **Working at your tables, review this control:**

§543.20

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

2. **Discuss and answer these questions:**
   - **Should the TGRA expand on this Control?**

     -and-

   - **Why or Why Not?**
3. **Participate in class discussion.**

IT-109 Auditing 543.20

IT-109 Auditing 543.20 Participant Guide

IT-109 Auditing 543.20

Information Technology Division

KEY POINTS

What to Expect

- Supervision - CFR543.20a
- Class II Gaming Logical and Physical Controls - CFR543.20c

- Physical Security - CFR543.20d
- Logical Security - CFR543.20e
- User Controls - CFR543.20f
- Remote Access - CFR543.20h
- Data Backups - CFR543.20j

KEY POINTS

What to Expect

- Software Downloads - CFR543.20k
- Verifying Downloads - CFR543.20l

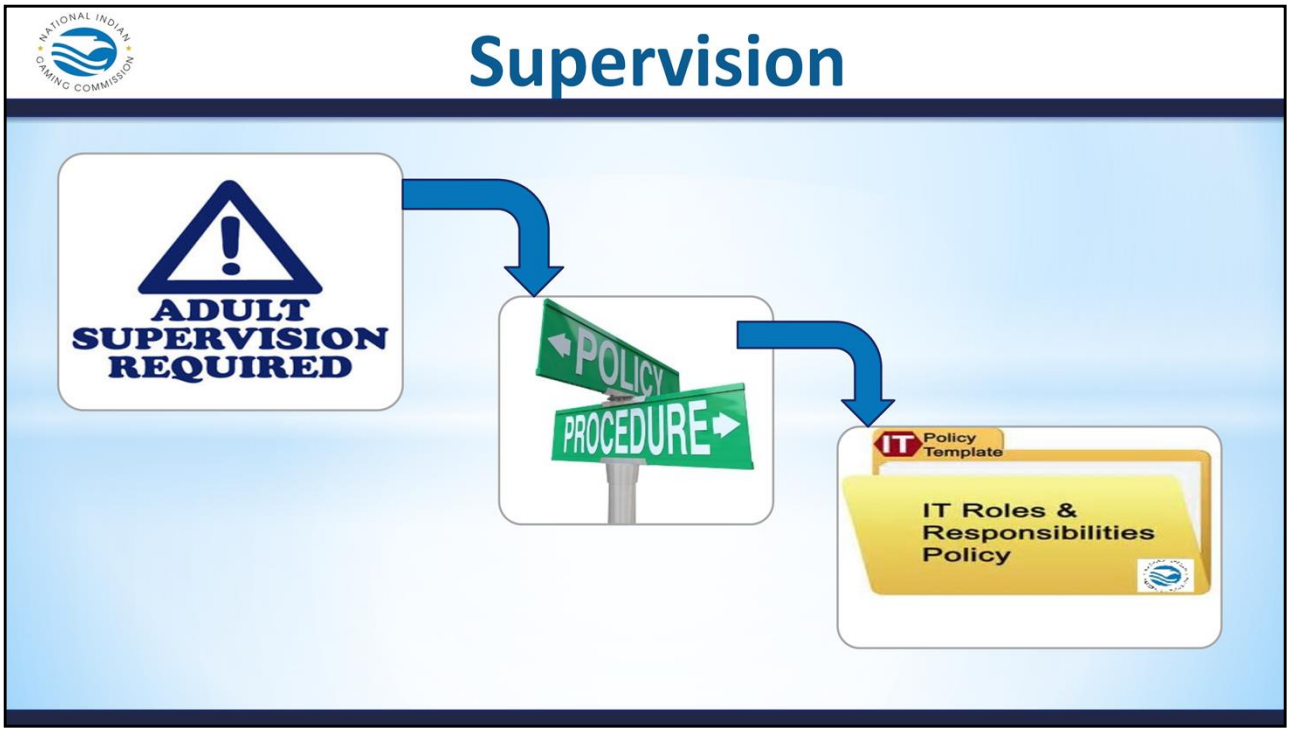
- Installation and/or modifications - CFR543.20g

- Incident monitoring and reporting - CFR543.20i

KEY POINTS


Where to Begin
Surveillance
Hotel Shops
Restaurants
Hotel Operations
Servers and Kiosks
Gaming
Casino Management System

KEY POINTS



KEY POINTS

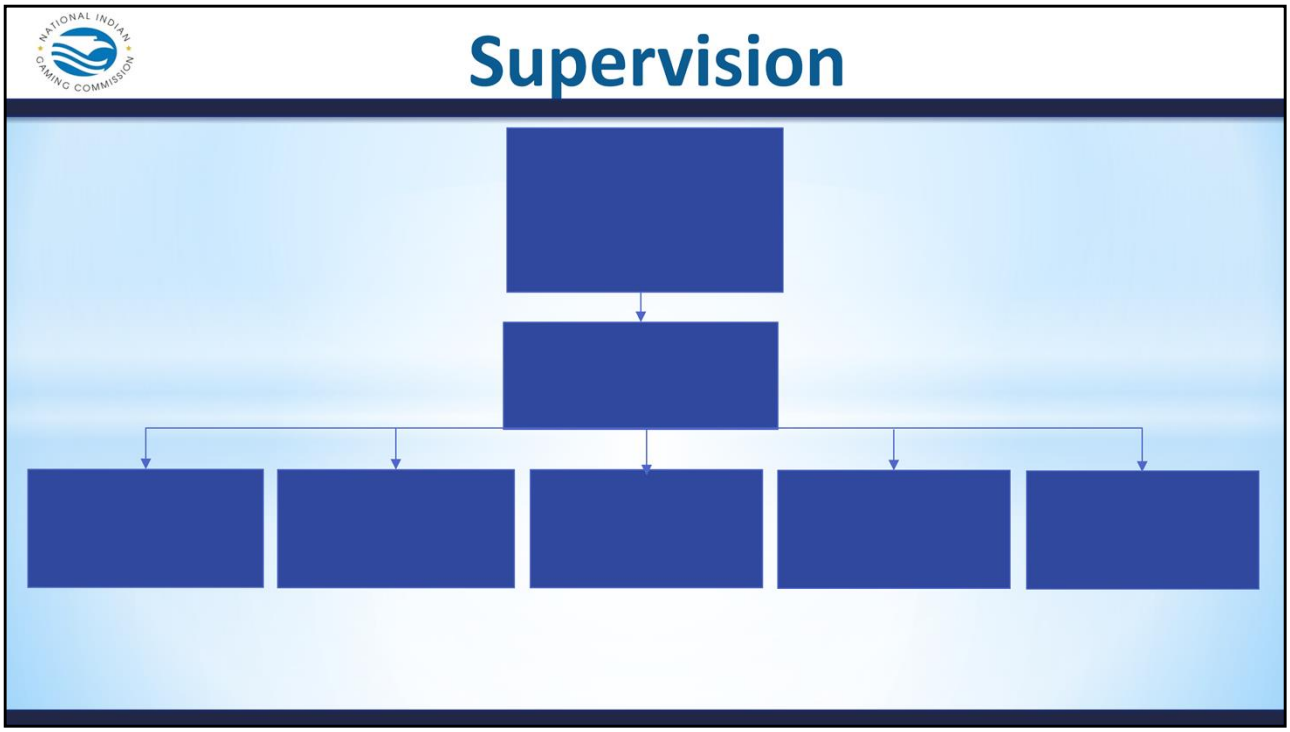
- Supervision includes – the action or process of watching and directing what someone does or how something is done. IT supervision ensures you have:
    - Policy and Procedures
    - IT Roles and Responsibilities
- Common Policy and Procedures:
- IT Roles and Responsibilities

Exercise 1 - Handout #1

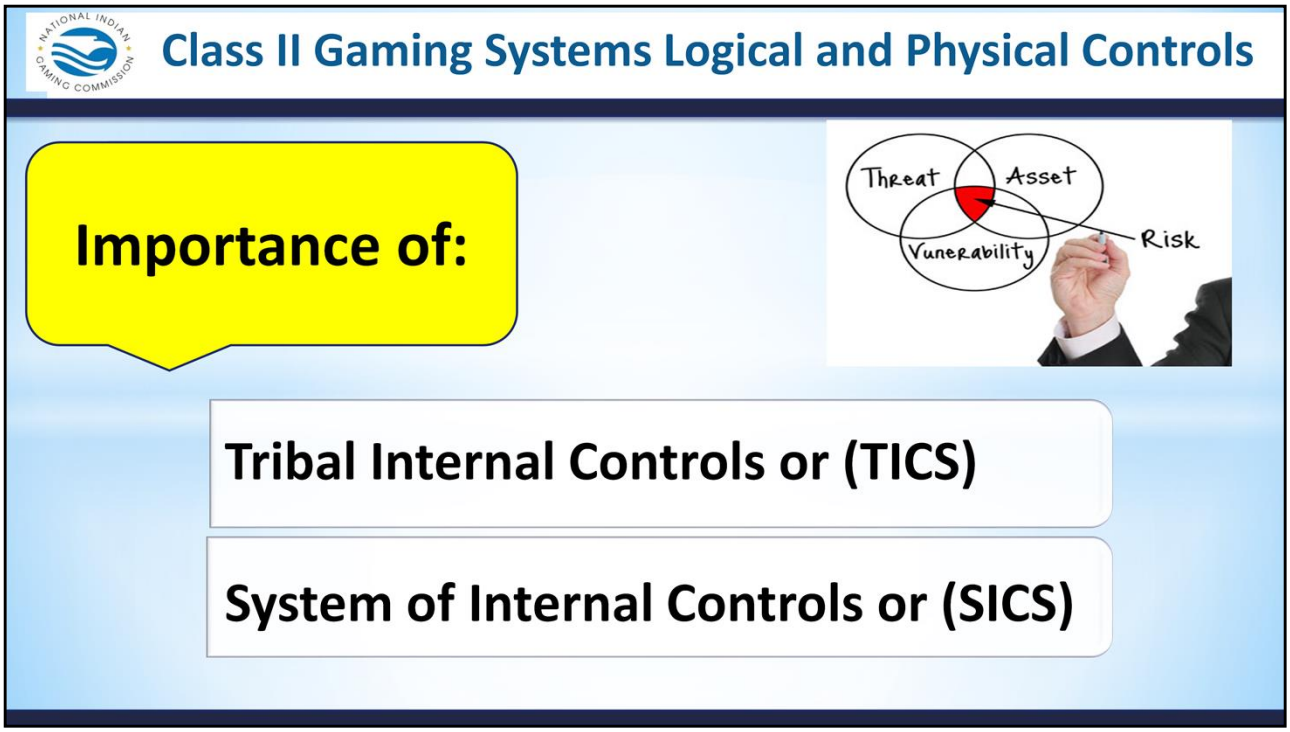
On Handout #1 - fill in the supervision hierarchy from top to bottom.

(Note: you have more job titles than spaces)

KEY POINTS



KEY POINTS



KEY POINTS

543.20 (c)(12) Are controls established and procedures implemented to ensure adequate: Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments? (Inquiry and review SICS)

What are the differences between TICS and SICS?

Ask Yourself

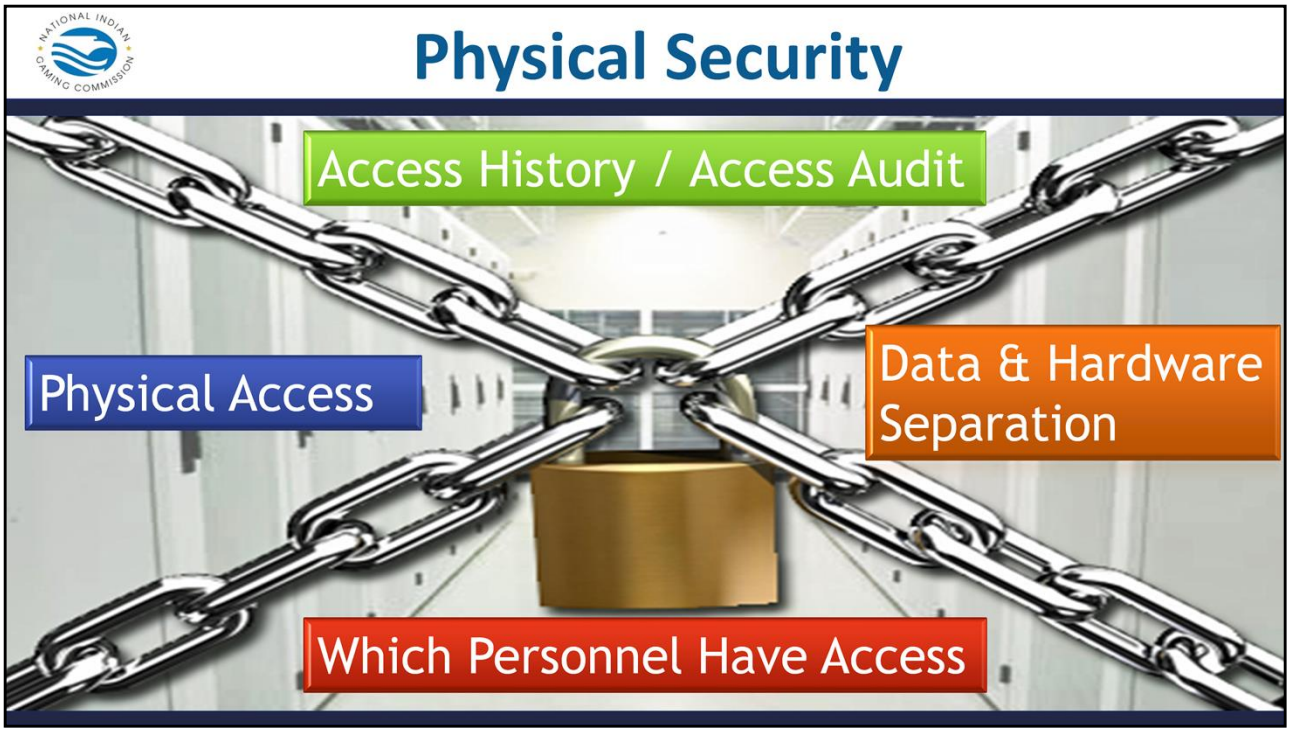
1. Who is in charge?
2. Should this person be independent of the class II system?
3. What methods (i.e. policy &/or procedure) are in place to detect errors or fraud?

KEY POINTS

Ask Yourself

4. Should that person have access to accounting, audit entries, or payouts?
5. Is there an audit procedure? How is the audit completed and how is it recorded?

KEY POINTS

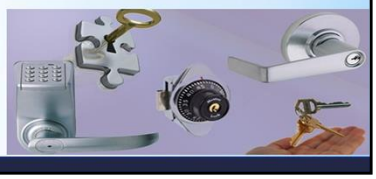


KEY POINTS

- *Look at physical access*.
- *Look at data and hardware separation.*
  - Are you housing different systems on the same server?
  - Is network equipment separated?
- *Look at which Personnel have access.*
  - Which IT people have access to what and when?
  - Which non-IT people have access to what and when?
- *Look at how often access history is audited and how often access privileges are audited?*
  - Depending on how access is logged, via a sign in sheet or via card key, how often is that log checked
  - How often are the access privileges of individuals audited?

Ask Yourself

1. Are the policy and procedures in place?
2. Who is responsible or has access?

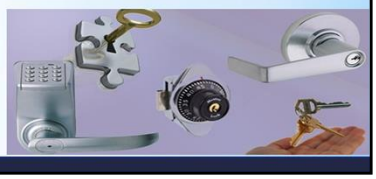


KEY POINTS

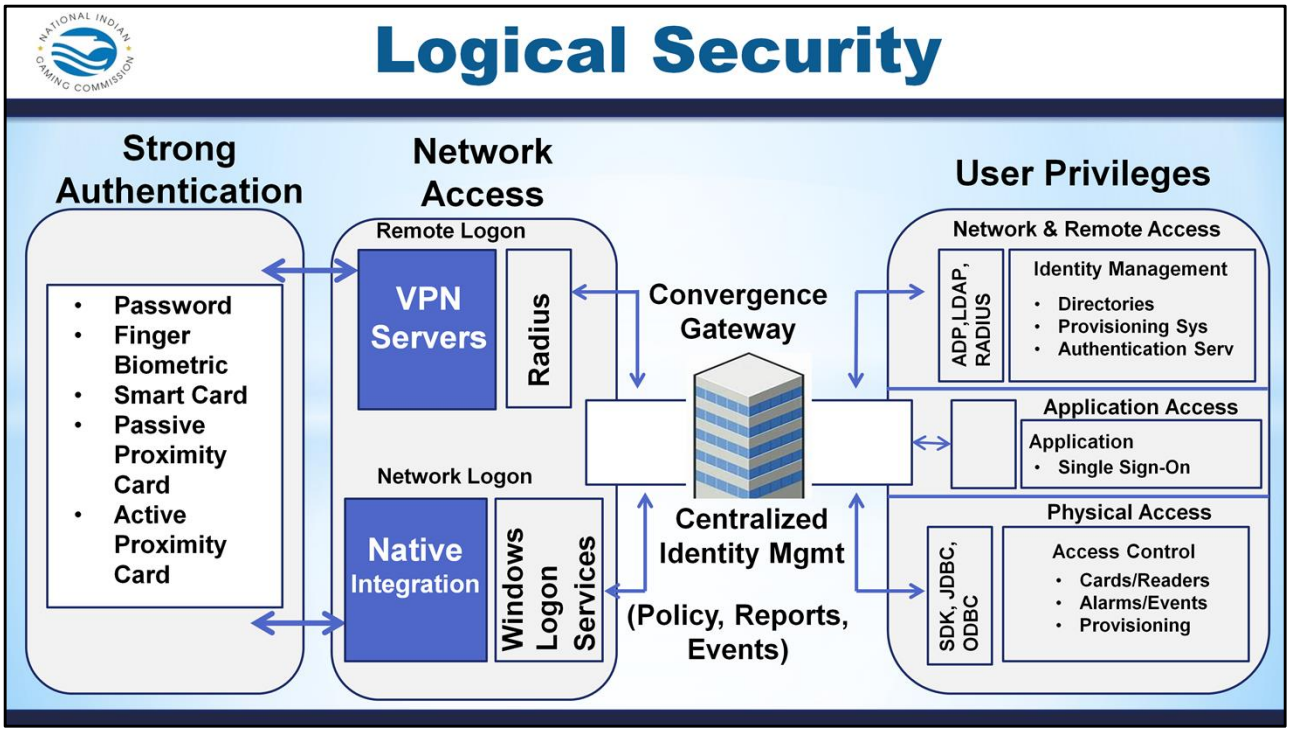
Ask Yourself

3. What group or who is recording and why?

4. Should that person be in the area?



KEY POINTS



KEY POINTS

543.20 (e)(17) Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: Systems' software and application programs? (Inquiry and review other – authorization lists)

543.20 (e)(18) Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

Data associated with Class II gaming? (Inquiry and review other – authorization lists)

- Look at SICS to protect all systems and ensure access is restricted

- Is there a process in place to grant or limit key access to various systems? (ie. Active Directory and Kerberos) –How are those utilized to give access to key servers, key folders, and key applications to users?
- Which IT personnel have access to each system? In a larger organization, you might have the floor operations support separate from the back-office operations support.
- Is the process of deciding who has access to what decided upon?
- Is the process of deciding access documented?

Ask Yourself

1. What policy and/or procedure exists?
2. Is there access to the data?
3. Who manages the rights and roles of those terminations?
4. Audit process for those records and how often reviewed?

KEY POINTS

Ask Yourself

5. Are robust passwords policies and procedures in place?
6. Are policy and procedures in place for network ports to be disabled?
7. What type of data encryption is in place?
8. Who ensures software is verified?

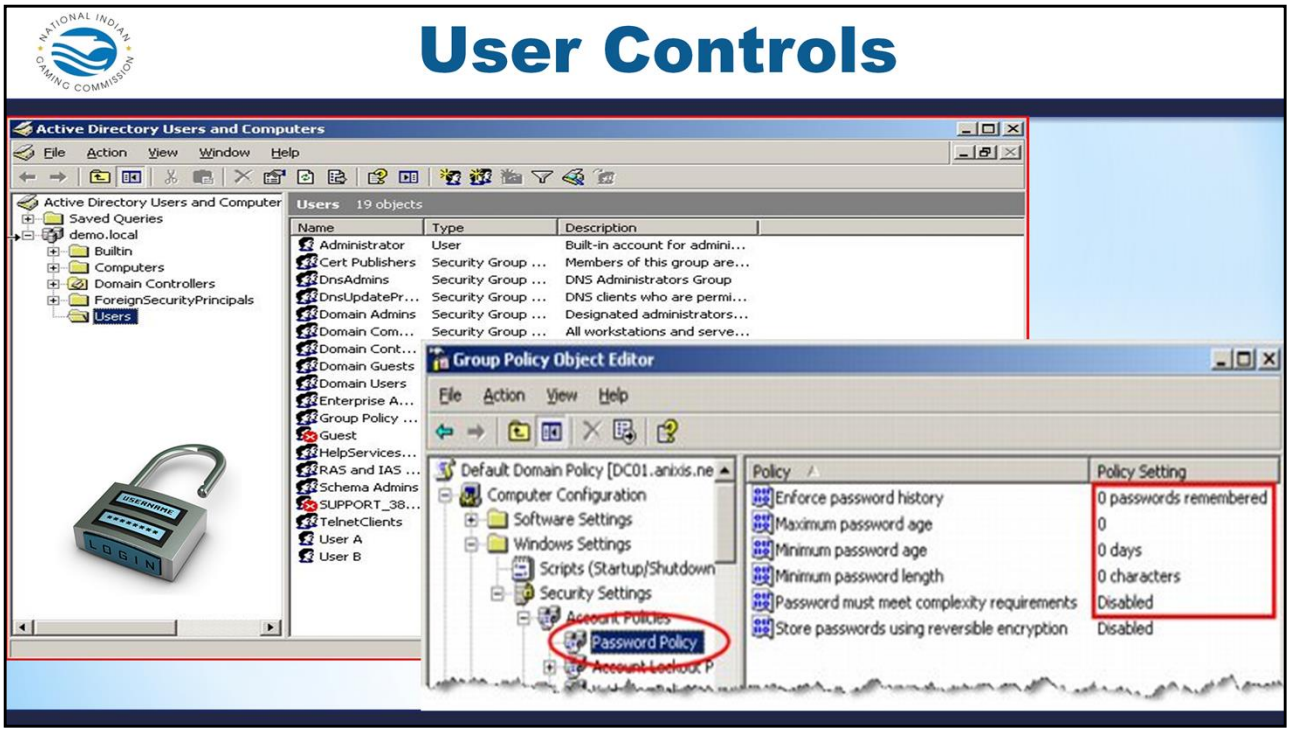
KEY POINTS

KEY POINTS

INSTRUCTIONS

Using all the terms at the bottom of the handout. Place the terms in the correct column.

KEY POINTS



KEY POINTS

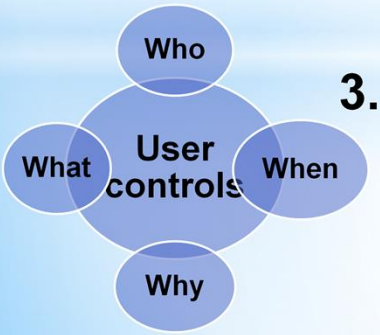
543.20 (f)(24) Are systems, including application software, secured with passwords or other means for authorizing access? (Inquiry and perform log-in tests on network system(s) and each stand-alone system)

543.20 (f)(32) Are lost or compromised access credentials deactivated, secured or destroyed within an established time period approved by the TGRA? State the time period _____. (Inquiry and review TGRA approval)

- *Look at SICS to make sure systems are protected with passwords or other means*
- *Look at SICS for lost and compromised access credentials* (ie. Terminated user policy, lost card policy)
- *Look at password complexity and reset period*

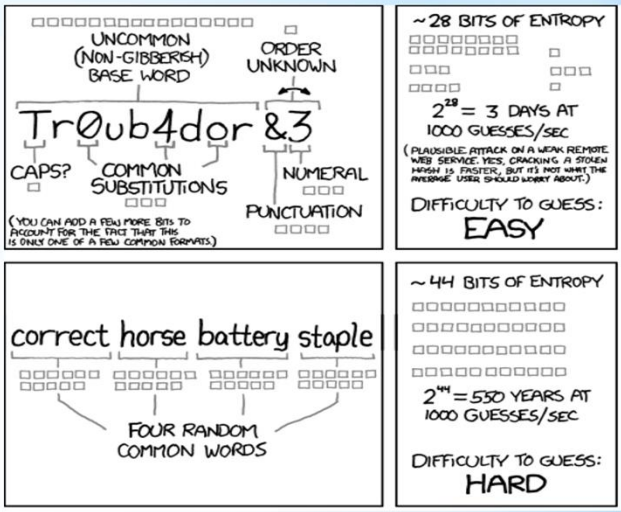
Ask Yourself

1. Who is assigned to control, update or modify system functions?
2. Are there roles and responsibilities for controls and are they approved by the TGRA?
3. Are user controls recorded with Who, When, Why and What was completed?



KEY POINTS

Passwords



Online password strength checking site:
http://howsecureismypassword.net/

Source:https://xkcd.com/936/

KEY POINTS

NIST standards for passwords updated in 2017: from 8 characters / 4 character types to short word phrases.

KEY POINTS

#41, #49

543.20 (h)(41) Is documentation for each remote access system support session maintained at the place of authorization? (Inquiry and review supporting documentation)

543.20 (h)(49) Is all remote access performed via a secured method? (Inquiry and review supporting documentation)

- Look at remote access logging

- Look at secured remote access

Remote Access

Monthly Logon/Logoff Report

Login	Logout	Group	Computer	Port	Remote IP	Username	Logon Type	Duration
Wed 2017-24-01 03:23:43PM	Wed 2017-24-01 04:25:44PM	Casino Name	DB Server	4025	10.70.158.129	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Thur 2017-24-01 03:23:43PM	Thur 2017-24-01 04:25:44PM	Casino Name	DB Server	4076	10.70.158.145	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Tue 2017-24-01 03:23:43PM	Tue 2017-24-01 04:25:44PM	Casino Name	DB Server	5284	10.70.158.121	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s

KEY POINTS

What is wrong with this picture?

Ask Yourself

Is there a Process for remote access that includes:

1. **When, Why and What was done during the remote access session and when the access was closed or terminated and by whom?**

KEY POINTS

Ask Yourself

Is there a Process for remote access that includes:

2. **Who was granted access, and who granted the access? License?**
3. **Is the remote access being done with a secure method? What is that method?**

KEY POINTS

Exercise 3 – Handout #3

KEY POINTS

INSTRUCTIONS

1. Break into groups and working together read each scenario, and identify the issue(s).
2. Locate the corresponding MICS standard using the IT Toolkit.
3. Then write a finding and include a recommendation.

KEY POINTS

KEY POINTS

Checklist #53, #55, #59, #61

543.20 (j)(53) Do controls include adequate backup, including, but not limited to, the following: Daily data backup of critical information technology systems? (Inquiry and review supporting documentation)

543.20 (j)(55) Do controls include adequate backup, including, but not limited to, the following: Secured storage of all backup data files and programs, or other adequate protection? (Inquiry and observation)

543.20 (j)(59) Do controls include recovery procedures , including, but not limited to, the following: Program restoration? (Inquiry and review supporting documentation)

- Look at backup schedule
- Look at security of backups
- Look at restoration methods
- Look at recovery process and testing of process

Ask Yourself

1. What is the backup process for all critical information and programs; is it stored in a means that is adequately protected from loss?
2. How often are the backups performed?

KEY POINTS

Ask Yourself

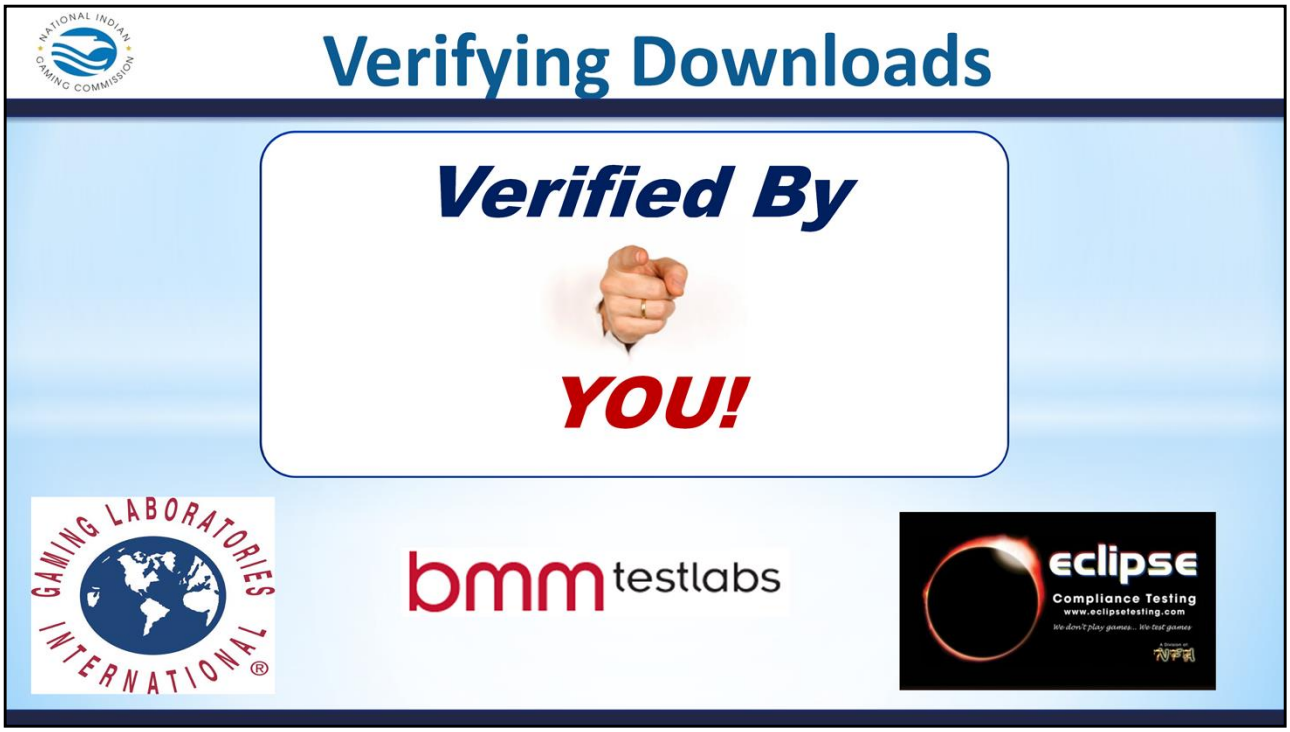
3. Is the information mirrored for redundancy and can the data be restored if required?
4. How often is this data backup process tested?

KEY POINTS

KEY POINTS

543.20(k)(63) Are downloads, either automatic or manual, performed in accordance with 25 CFR 547.12? (Inquiry and review SICS)

1. Acceptable means of transporting APPROVED content
2. Use secure methodologies that will deliver data without alteration or modification
3. Downloads during operational periods will not affect game play
4. Must not affect integrity of accounting data
5. C2 gaming MUST be capable of providing
    - Time & date of initiated download
    - Time & date of completed download
    - C2 gaming system components to which software was downloaded
    - Versions of download package and any software. Logging unique software signature
    - Outcome of any software verification (Success or Failure)
    - Name and ID number, or other unique identifier, of any individuals conducting or scheduling a download



KEY POINTS

Verifying downloads – Software on C2 gaming system MUST be capable of verification by C2 Gaming system using a software signature verification method that meets 547.8(f)

543.20(l)(64) Following the download of any Class II gaming system software, does the Class II gaming system verify the downloaded software using a software signature verification method? (Inquiry and review supporting documentation)

- *Look at download process*
- *Look at signature verification*
- *Look at best practices.* *(Remember 542.16)*

KEY POINTS

543.20(g)(36) Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum: The date of the installation or modification? (Inquiry and review supporting documentation)

543.20(g)(38) Are records kept of all new installations and/or modifications to Class II gaming systems that include the following, at a minimum: Evidence of verification that the installation or the modifications are approved? (Inquiry and review supporting documentation)

- *Look at records and versions of installs* - Is there a written record of the install
- *Look at records of all new installations and modifications* - Is there proof of the software verification?
- *Look at change management process*
    - Is there a documented process for testing new software or hardware
    - Is there a documented process for incorporating new software and hardware into the destination environment?
- Is there a process for vetting approved vendors?

Ask Yourself

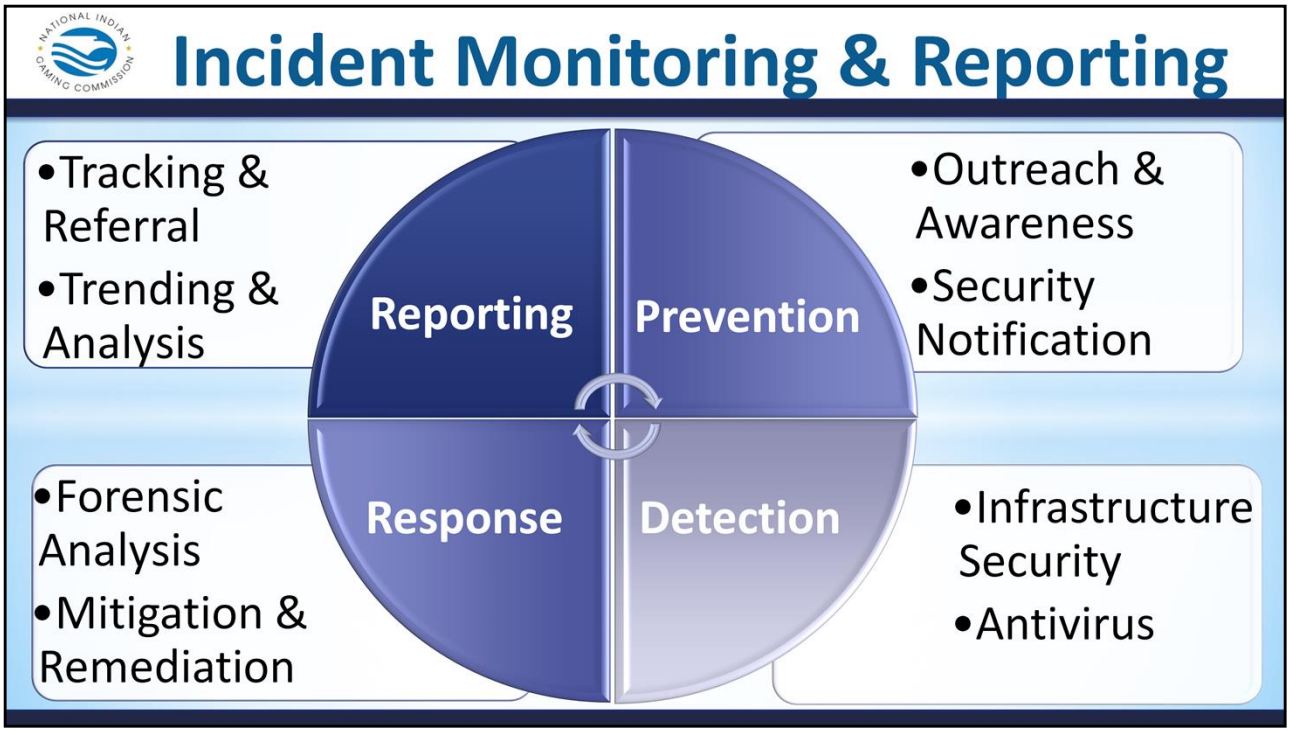
1. Are only authorized and approved systems being installed or modified and is it being verified to a checklist?
2. Are these actions being recorded, if so with Whom, When, Why and What was accomplished?

KEY POINTS

Ask Yourself

3. **Are there instruction manuals or booklets that describes the system and how its maintained?**

KEY POINTS



KEY POINTS

Incident Monitoring & Reporting

543.20(i)(51) Are all security incidents responded to within the established time period approved by the TGRA? State the time period_____.

(Inquiry, review TGRA approval, and review supporting documentation)

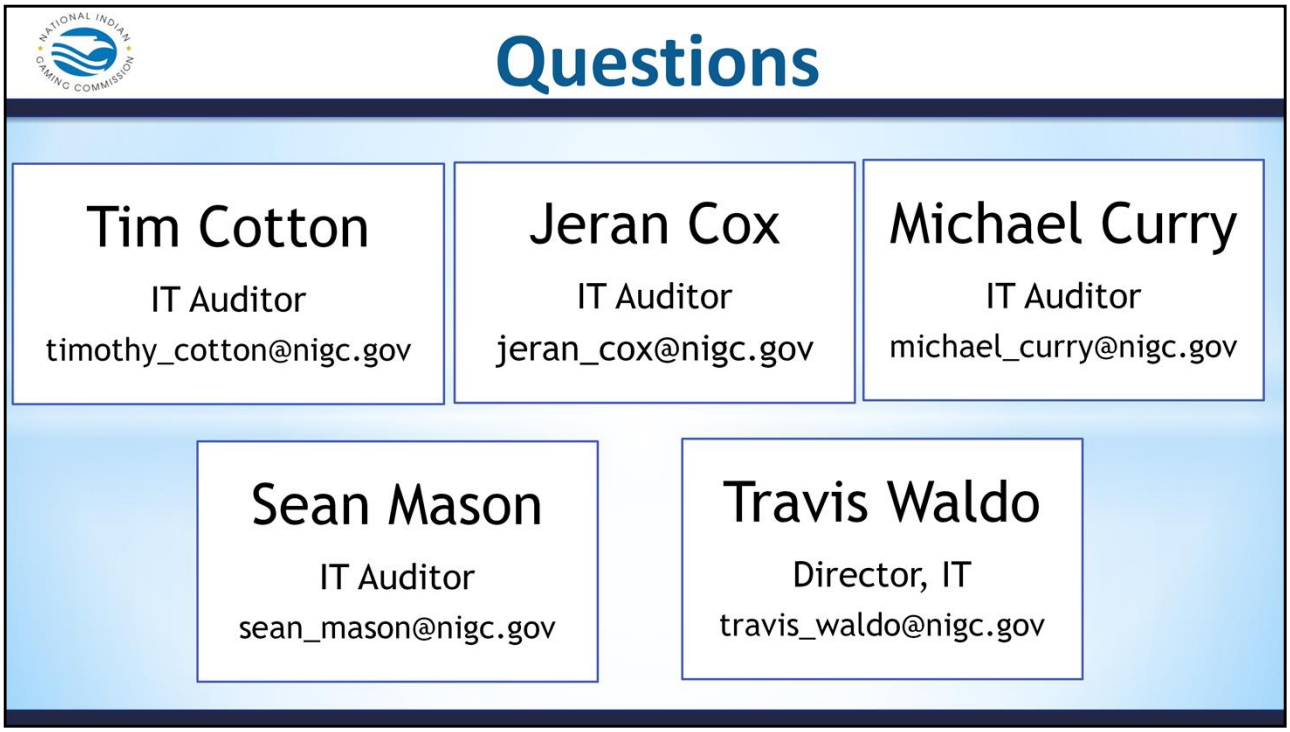
- What are the processes for responding to monitoring, investigating, resolving, documenting, and reporting security incidents?
    - Is there a documented response time period for incidents?
    - Is there a tracking system for **reporting** incidents and are they being utilized for data analysis?
    - What steps for outreach and notification are being taken to promote **prevention**?
- What **detection** methods are in place?
- What is the **response** system

Ask Yourself

1. What are the policies and/or procedures for responding to, monitoring, investigating and resolving all security incidents that is approved by the TGRA?
2. What time period has been established with the TGRA for supporting documentation to be supplied?

KEY POINTS

Ask Yourself – Incident Monitoring and Reporting

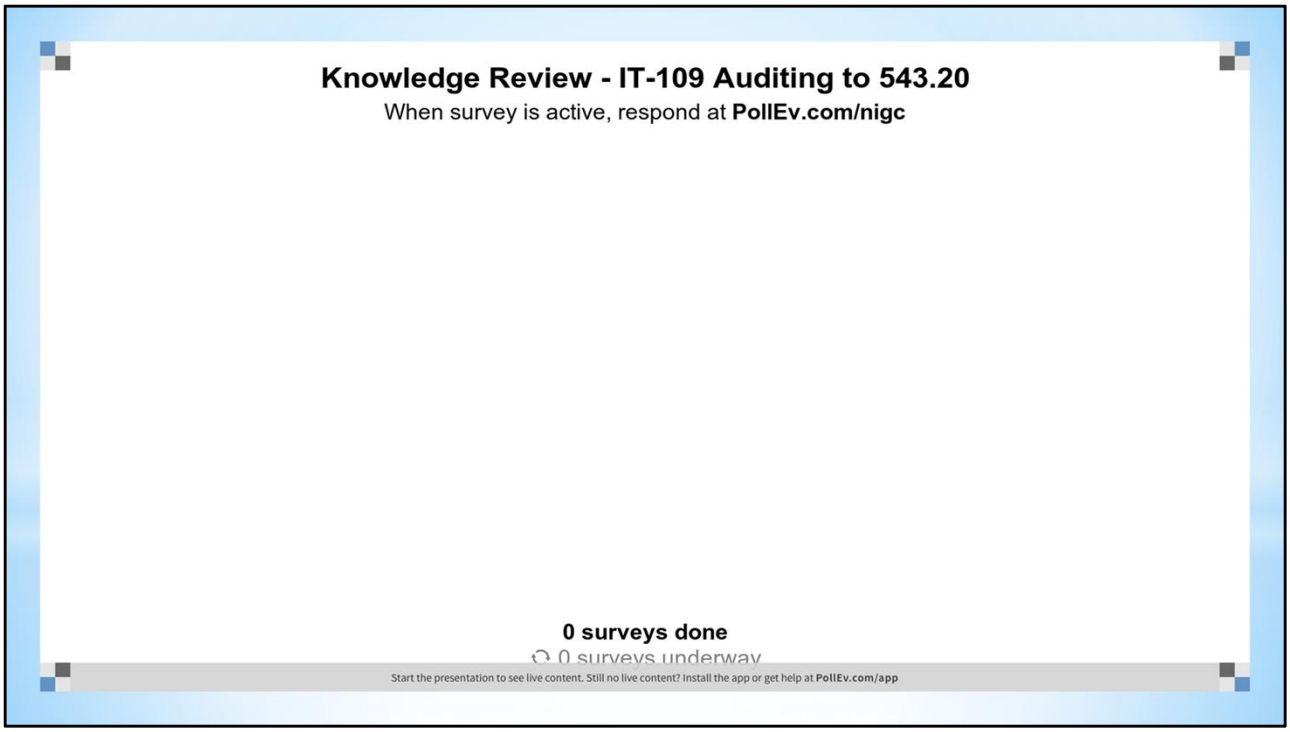

Questions
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov
Jeran Cox
IT Auditor
jeran_cox@nigc.gov
Michael Curry
IT Auditor
michael_curry@nigc.gov
Sean Mason
IT Auditor
sean_mason@nigc.gov
Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS

Course Evaluation

- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciate and allow us to improve your experience

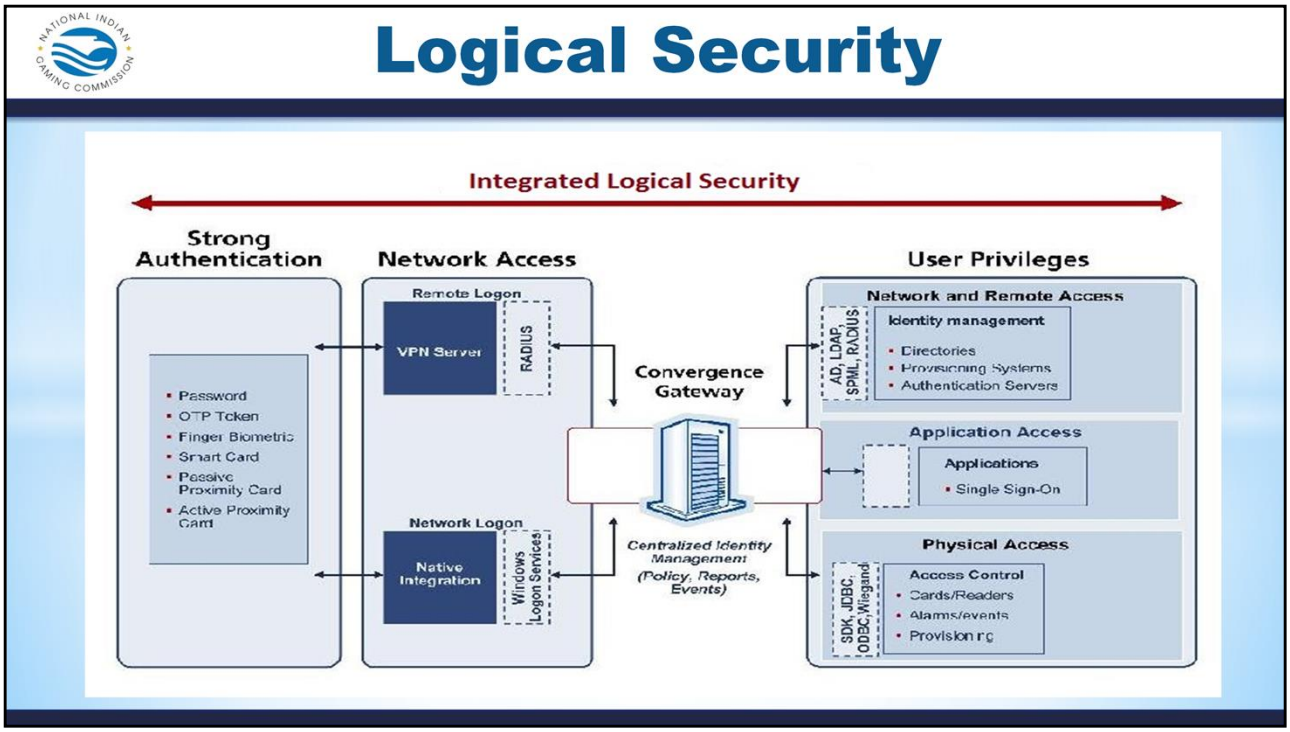
KEY POINTS



KEY POINTS

Poll Title: Knowledge Review - IT-109 Auditing to 543.20

https://www.polleverywhere.com/surveys/Qdj8myfmA



KEY POINTS

Logical security – focus #17 and #18

543.20 (e)(17) Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: Systems' software and application programs? (Inquiry and review other – authorization lists)

543.20 (e)(18) Are controls established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

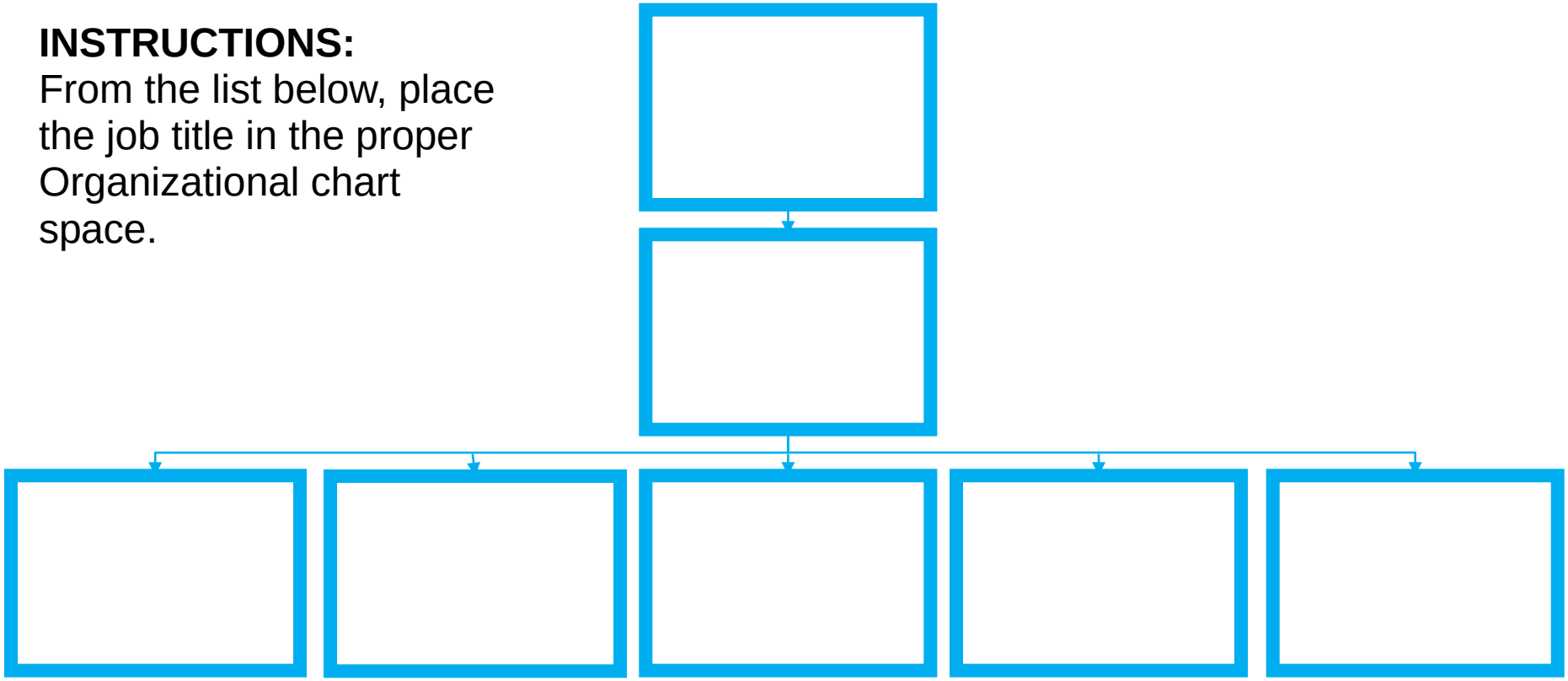
Data associated with Class II gaming? (Inquiry and review other – authorization lists)

Look at SICS to protect all systems and ensure access is restricted

- Is there a process in place to grant or limit key access to various systems? – For example: Active Directory and Kerberos are two of the most common authentication services. But how are those utilized to give access to key servers, key folders, and key applications to users? Which IT personnel have access to each system? In a larger organization, you might have the floor operations support separate from the back-office operations support.
- Is the process of deciding who has access to what decided upon? – For example: When an individual requests access to a room or to an application how is it determined if they get it or not? Do you need a manager approval? Do you accept ANY manager's approval? Is there a process not just to add access but to grant or deny?
- Is the process of deciding access documented? – For example: When the head of IT leaves the org. will anyone understand the process when they are gone? And, will they do it the same way?

HANDOUT #1 – Exercise 1

INSTRUCTIONS:
From the list below, place the job title in the proper Organizational chart space.



Helpdesk Manager
Application Developer
Software Development Manager
Chief Information Officer
Web Development Manager
Telecom Manager

IT Director
Telecom Technician
Desktop Support
Web Developer
Database Administrator
Network Manager

Handout #2 – Exercise 2

INSTRUCTIONS:

Place the terms in the correct column.

Physical security:	Logical security:
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Protects Computer Software

User IDs

Intrusion Detection

Smart Cards

Alarms

Cameras

Electronic Access Controls

Port management

Administration Access Controls

Password Authentication

Information Technology – Audit
25 CFR 543.20 Toolkit

Version 1.0

NIGC Compliance Division

NIGC Information Technology Audit–25 CFR 543.20 Toolkit

Over twenty five years ago Congress adopted the Indian Gaming Regulatory Act (IGRA) to provide a statutory basis for gaming by Indian tribes. The National Indian Gaming Commission (NIGC) was created by IGRA to regulate gaming activities conducted by sovereign Indian tribes on Indian lands. The mission of the NIGC is to fully realize IGRA's goals of: (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. One of the primary ways the NIGC does this is by providing training and technical assistance to Indian tribes and their gaming regulators.

The National Indian Gaming Commission (NIGC) is pleased to present this Toolkit to all Compliance and Auditing staff. This reference guide is intended to assist IT Auditor(s), Gaming Commissioner(s) and Operations personnel in the performance of measuring compliance of their operation(s) with 25 CFR 543.20. The toolkit is designed to provide each standard as it relates to 543.20, the language of the standard, the intent of the standard, and then a recommended testing step which will ensure minimum regulatory compliance.

This Toolkit is designed to meet the minimum requirements of the NIGC MICS and does not take into account operations Tribal Internal Controls Standards (TICS) and or System of Internal Controls Standards (SICS), which may require further testing. The NIGC encourages Operations to develop standards that exceed the Minimum Internal Control Standards , because each operation is unique, therefore a robust set of controls is warranted.

If you have questions or comments about this guide, please contact the NIGC Compliance Division at **training@nigc.gov**. For more information, visit the NIGC website at **http://www.nigc.gov.**

Citation	Language	Intent and Testing
§ 543.20 (a-b)		
543.20 (a)(1)	*Supervision.* (1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.	**Intent:** To ensure that the TICS identify who is the supervisory agent in the department and is responsible for ensuring the IT Department is operating in accordance with established policy and procedures. **Testing: 1.** Review TICS to identify controls with respect to the supervision of the IT Department. **2.** Identify any additional controls required by the TGRA with regards to supervision. **3.** Review SICS to ensure that operations have identified and implemented controls with regards to the TGRA requirements in their TICS.
543.20(a)(2)	The supervisory agent must be independent of the operation of Class II games.	**Intent:** To ensure proper segregation of duties that the IT supervision is independent of all Class II Games. Best practices suggests that the IT department should be independent of all casino departments and should report directly to the General Manager. **Testing: 1.** Review Information Technology Organizational Chart. **2.** Inquire with IT supervision to determine who they report to.
543.20(a)(3)	Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.	**Intent:** To ensure that IT personnel are not to be assigned conflicting roles, i.e., financial, accounting and gaming responsibilities that cannot be effectively monitored for the detection of fraud or the concealment of procedural errors. **Testing: 1.** Review Human Resources job descriptions in IT personnel files in addition to IT user groups and accounts. **2.** Flag instances of computerized IT access to financial, accounting or gaming roles.

Citation	Language	Intent and Testing
§ 543.20 (a-b)		
543.20(a)(4) (i-iii)	Information technology agents having access to Class II gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to: (i) Financial instruments; (ii) Accounting, audit, and ledger entries; and (iii) Payout forms.	**Intent:** IT personnel who possess access to Class II gaming shall not have access to or signatory authority over financial instruments, accounting, audit, ledger entries and payout forms. **Testing: 1.** Review system user access accounts of IT personnel for financial, accounting, ledger and payout form access. **2.** Review physical payout forms for winners. **3.** Review SICS to verify that IT personnel are not authorized to sign
543.20(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. **Testing:** Review gaming operations architectural plans and computerized network system design layout and applications system inventory.

Citation	Language	Intent and Testing
§ 543.20 (c)		
543.20 (c)	Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:	**Intent:** To ensure that operational SICS have identified and implemented controls with regards to the TGRA requirements in their TICS. **Testing:** Review IT TICS, SICS and Policies and Procedures.
543.20(c)(1)	Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;	**Intent:** To ensure both physical and logical access to critical computerized environments, networks and application system are restricted to authorized users. **Testing:** Review IT TICS, SICS and Policies and Procedures for verification of controls in place for the control of both physical and logical access to the information technology environment used in conjunction with Class II gaming by reviewing the user access list against the current HR list.
543.20(c)(2)	Physical and logical protection of storage media and its contents, including recovery procedures;	**Intent:** To ensure that stored and archived financial, accounting and gaming data can be readily restored to the gaming operations 'live' environment during or after a critical system failure. **Testing: 1.** Review IT TICS, SICS and Policies and Procedures for data recovery controls and processes. **2.** Review data backup and recovery scheduling, testing and physical assessment of the data storage facility.

Citation	Language	Intent and Testing
§ 543.20 (c)		
543.20(c)(3)	Access credential control methods;	**Intent:** To ensure that only properly vetted and authorized personnel have access to the gaming operations secured logical and physical environments. **Testing:** Review IT TICS, SICS and Policies and Procedures for effective logical and physical access control methods and reviewing the user access list against the current HR list.
543.20(c)(4)	Record keeping and audit processes; and	**Intent:** To ensure that administrative bookkeeping and accurate and timely documentation supporting audit processes is maintained. **Testing:** Review SICS and audit results with findings from previous internal and external audits and also any records kept by the IT operation.
543.20(c)(5)	Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.	**Intent:** To ensure that technical departments and technical personnel are restricted from access to financial instruments. **Testing:** Review SICS and organizational chart structure. Perform review of financial logical access permissions and authorizations of technical personnel. Flag access accounts authorizing IT personnel to financial instruments.

Citation	Language	Intent and Testing
§ 543.20 (d-e)		
543.20(d)	*Physical security.* (1) The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.	**Intent:** To ensure that the information technology environment and supporting environments are maintained in a secured physical location. Access is to be restricted to authorized personnel in a secured physical location that is accessible only to authorized personnel. **Testing:** Conduct physical walkthrough inspection noting the access / denial methods to restrict physical access to critical locations, i.e., HID card, hard-key, biometrics, pin code, password, etc.
543.20(d)(2)	Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.	**Intent:** To ensure that those who are recipients of the security access tools, are not the same as those who authorize, manage and assign the security access tools. **Testing: 1.** Verify roles, responsibilities and organizational positions of the personnel responsible for physical access management. **2.** Note any potential independent conflicts and effectiveness of managerial oversight.
543.20(d)(3)	Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.	**Intent:** To ensure only authorized agents gain access to secured physical locations, in accordance with established Policies and Procedures to include maintaining and updating a ledger or listing of those agents granted access privileges. **Testing:** Review SICS, TICS, Policies and Procedures also spot check any access logs and review of management's approved Authorized User Access Listing(s).

Citation	Language	Intent and Testing
§ 543.20 (d-e)		
543.20(d)(4)	Network Communication Equipment must be physically secured from unauthorized access.	**Intent:** To ensure the network infrastructure and equipment, organizational intranet and all incoming and outgoing network communications are secured from unauthorized access. **Testing: 1.** Verify the software application affected has the proper physical security measures in place that can be tested over the Network Communication Equipment environment. **2.** Obtain network communications diagrams to include flow of internal and external data flows, hardware topology and system application flows. **3.** Perform physical walkthrough of network communications architecture and facilities to include surveillance and security measures.
543.20(e)(i-iii)	*Logical security.* (1) Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured: (i) Systems' software and application programs; (ii) Data associated with Class II gaming; and (iii) Communications facilities, systems, and information transmissions associated with Class II gaming systems.	**Intent:** To ensure that all organizational software systems and data and communication systems are restricted from unauthorized access. **Testing:** Verify the effectiveness of security and operational controls supporting the physical and logical segregation of the organizational intranet and external internet. This can be accomplished by reviewing diagrams and technical documents along with any logs
543.20(e)(2)	Unused services and non-essential ports must be disabled whenever possible.	**Intent:** To ensure the deactivation or isolation of unused services and non-essential communication and computer ports. Non-essential ports are to be disabled whenever possible. **Testing:** Review IT Policies and Procedures and perform walkthrough of open ports in vacated offices, cubicles, conference rooms, etc.

Citation	Language	Intent and Testing
§ 543.20 (e-f)		
543.20 (e)(3)	Procedures must be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access, and logged.	**Intent:** To ensure that procedures are in place that all activity performed on the computerized system is recorded and / or logged. **Testing:** Review SICS and IT Policies and Procedures. Review change management documentation, i.e., work requests, job orders, work orders and review access logs.
543.20(e)(4)	Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.	**Intent:** To ensure that electronic communications, to include wireless, copper wire, satellite or cellular, is logically secured from unauthorized access. **Testing: 1.** Review TICS and SICS and Policies and Procedures. **2.** Verify that network security measures are in place to include any necessary routers, firewalls, switches and encryption. **3.** Verify that software upgrades to communications equipment is current.
543.20(f)	*User controls.* (1) Systems, including application software, must be secured with passwords or other means for authorizing access.	**Intent:** To ensure that only authorized system account holders have access to computerized systems, including application software. **Testing: 1.** Verify that all critical accounting, financial and gaming systems are secured with passwords or other means to limit logical system access. **2.** Review user access listings.

Citation	Language	Intent and Testing
§ 543.20 (e-f)		
543.20(f)(2)	Management personnel or agents independent of the department being controlled must assign and control access to system functions.	**Intent:** To ensure that procedures are in place that all activity performed on the computerized system is recorded and / or logged. **Testing:** Review SICS and IT Policies and Procedures. Review change management documentation, i.e., work requests, job orders, work orders and review access logs.
543.20(f) 3) (i-iii)(A-C)	Access credentials such as passwords, PINs, or cards must be controlled as follows: (i) Each user must have his or her own individual access credential; (ii) Access credentials must be changed at an established interval approved by the TGRA; and (iii) Access credential records must be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user: (A) User's name; (B) Date the user was given access and/ or password change; and (C) Description of the access rights assigned to user.	**Intent:** To ensure that all authorized access holders meet minimum credential requirements to retain their access permissions. **Testing: 1.** Review TICS, SICS and group user account holders. **2.** Review administrator account parameter settings for group and individual user access settings.

Citation	Language	Intent and Testing
§ 543.20 (f-g)		
543.20 (f)(4)	Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.	**Intent:** To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. **Testing:** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.
543.20(f)(5)	Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.	**Intent:** To ensure that access credentials of terminated users are deactivated in the minimum time period stated by the TGRA. **Testing: 1.** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee, IT Management and Human Resources action when compromised credentials are reported. **2.** Review user access lists for former employees
543.20(f)(6)	Only authorized agents may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.	**Intent:** To ensure that terminated, transferred or resigned personnel accounts are only accessible by, or approved by, TGRA authorized agents. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures regarding User Network Security and Access activity. **2.** Verify appropriate access by comparing access logs/permissions to TICS/SICS/Policies & Procedures.

Citation	Language	Intent and Testing
§ 543.20 (f-g)		
543.20(g)	*Installations and/or modifications*. (1) Only TGRA authorized or approved systems and modifications may be installed.	**Intent:** To ensure that organizational personnel must first seek approvals of TGRA and IT Management prior to the introduction of outside software or modifications to the network or computerized systems. **Testing:** Review TICS, SICS and IT Policies and Procedures. Review a sampling of previous change management request forms for proper approvals and signatures.
543.20(g)(2) (i-iv)	Records must be kept of all new installations and/or modifications to Class II gaming systems. These records must include, at a minimum: (i) The date of the installation or modification; (ii) The nature of the installation or change such as new software, server repair, significant configuration modifications; (iii) Evidence of verification that the installation or the modifications are approved; and (iv) The identity of the agent(s) performing the installation/modification.	**Intent:** To ensure that evidential and supporting documentation is retained for all new installations and modifications to Class II gaming systems. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures regarding change management and asset management. **2.** Review sampling of records retained of records of installations and / or modifications.

Citation	Language	Intent and Testing
§ 543.20 (g-i)		
543.20 (g)(3)	Documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.	**Intent:** To ensure that documentation accompanying new or used hardware is retained describing said system in use and it's proper operation, to include hardware systems. **Testing: 1.** Review sampling of supporting system user manuals, specification sheets, build sheets, etc., and a walkthrough or the secured location(s) where maintained. **2.** Documentation may be stored or archived in an approved documentation storage file onsite, or on the vendor / manufacturers website.
543.20(h)(1) (i–vii)	*Remote access.* (1) Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include: (i) Name of agent authorizing the access; (ii) Name of agent accessing the system; (iii) Verification of the agent's authorization; (iv) Reason for remote access; (v) Description of work to be performed; (vi) Date and time of start of end-user remote access session; and (vii) Date and time of conclusion of end-user remote access session.	**Intent:** To ensure remote access connections are secure, approved and accurately recorded / logged. **Testing:** Review SICS, TICS and IT Policies and Procedures and sampling of remote access session logs. Remote access logs at a minimum must provide bullet points (i) through (vii).

Citation	Language	Intent and Testing
§ 543.20 (g-i)		
543.20(h)(2)	All remote access must be performed via a secured method.	**Intent:** To ensure that lost or stolen user access credentials are deactivated in the minimum time period stated by the TGRA. **Testing:** Review TICS, SICS, Policies and Procedures and Employee Manuals for employee and IT Management action when compromised credentials are reported.
543.20(i)	*Incident monitoring and reporting.* (1) Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.	**Intent:** To ensure expedient and appropriate response to computerized incidents, faults, errors or cyber attacks. **Testing: 1.** Review TICS, SICS, IT Policies and Procedures and review sampling of Incident Responses and the courses of action taken. **2.** Review relevant work orders, job orders or work requests completed to address the incident(s).
543.20(i)(2)	All security incidents must be responded to within an established time period approved by the TGRA and formally documented.	**Intent:** To ensure all security incidents are responded to and addressed within a practical time period to mitigate the associated incident risk. **Testing:** Review TICS, SICS, or P&P for a time period established by security incidents should be responded to as soon as possible from the moment of notification.

Citation	Language	Intent and Testing
§ 543.20 (j-l)		
543.20 (j)(1) (i-v)	*Data backups.* (1) Controls must include adequate backup, including, but not limited to, the following: (i) Daily data backup of critical information technology systems; (ii) Data backup of critical programs or the ability to reinstall the exact programs as needed; (iii) Secured storage of all backup data files and programs, or other adequate protection; (iv) Mirrored or redundant data source; and (v) Redundant and/or backup hardware.	**Intent:** To ensure that adequate data and software backup controls are in place to support expedient organizational data restoration. **Testing: 1.** Review TICS, SICS and data backup scheduling processes for all application systems hosted by the gaming operation. **2.** Verify the secured storage of all backup data files and backup media.
543.20(j) (2)(i-iii)	Controls must include recovery procedures, including, but not limited to, the following: (i) Data backup restoration; (ii) Program restoration; and (iii) Redundant or backup hardware restoration.	**Intent:** To ensure that organizational controls include data, program, hardware and network restoration and recovery procedures. **Testing: 1.** Review SICS, TICS and Information Technology Policies and Procedures regarding management of system recovery processes. **2.** Review recovery and restoration documentation to include data, programs and redundant hardware.
543.20(j)(3)	Recovery procedures must be tested on a sample basis at specified intervals at least annually. Results must be documented.	**Intent:** To ensure that organizational recovery procedures are tested annually by Information Technology personnel and IT Management. **Testing: 1.** Review TICS, SICS and IT Policies and Procedures to routine recovery procedures. **2.** Review annual recovery testing documentation for performance and results of recovery test.

Citation	Language	Intent and Testing
§ 543.20 (j-l)		
543.20(j)(4)	Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.	**Intent:** To ensure that backup data files and recovery components are managed to at least the same stringent level of security as the systems for which they are supporting. **Testing:** Perform walkthrough of the backup data files physical location for security access restrictions, surveillance monitoring, fire suppression systems and HVAC equipment function.
543.20(k)	Software downloads. Downloads, either automatic or manual, must be performed in accordance with 25 CFR 547.12.	**Intent:** To ensure that software downloaded to the gaming operation from outside sources, either automatic or manual, is in strict compliance with 25 CFR 547.12. **Testing: 1.** Review TICS, SICS and Policies and Procedures. Verify that software downloads are delivered through secure methods. **2.** Review Class II system records to verify that the Class II system has recorded the (a) date and time of the initiation and (b) completion of any download, (c) the components that received it, (d) the version of the download package and any software downloaded, (e) status of the download attempt (i.e., success or failure), (f), unique identifier of individual conducting or scheduling the download.
543.20(l)	*Verifying downloads.* Following download of any Class II gaming system software, the Class II gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, the TGRA must confirm the verification.	**Intent:** To ensure that following the download of Class II gaming system software, the gaming system must verify the download with a software signature verification method, approved by the TGRA. **Testing: 1.** Review TICS, SICS and Policies and Procedures and verify that software downloads meet requirements. **2.** Review records to confirm TGRA verification of software

THIS PAGE INTENTIONALLY LEFT BLANK

25 CFR 543.20 Toolkit

Version 1.0

NIGC Compliance Division

National Indian Gaming Commission

Toolkit Exercise

Break into groups, working together read each scenario, and identify the issue(s) and locate the corresponding MICS standard using the IT Toolkit. Then write a finding and include a recommendation.

Scenario #1:

Vendor Z has an always on connection between their service center and the Class II server housed in the tribe's server racks. This connection has been approved by IT Security and by the Gaming Commission since 10/03/2012. The vendor has a staff of properly licensed database admins that utilize the connection to perform daily manual database backups and trouble shooting at the tribe's request. On 01/15/2014 Erik Magnus, the external auditor, asks for a log of all remote access to that server from 12/01/2013 to 12/31/2013. He is given a screenshot of windows usernames and logins for the time period.

MICS REFERENCE: _____

FINDING:

_____
_____
_____
_____
_____
_____
_____

RECOMMENDATION:

_____
_____
_____
_____
_____
_____

Handout #4 – Exercise 2

Scenario #2:

The IT Auditor reviewed the Casinos SICS, mapped the card access (ex. HID Card) and key control process. Based on review of the Casino SICS the Auditor noted that access to physical locations are controlled by a combination of two security measures; card access and physical keys. Both the card access and keys are controlled by software. The IT Manager has access to the key box software in order to change an individual's user group. Access to the card access software is limited to the IT Manager, General Manager and the CEO. The Auditor conducted an interview with the IT Manager and learned that card access is reviewed by the IT Manager when there is a change in job status (i.e. new hire, department transfer or termination). Additionally, an IT audit is performed twice a year. Further the Auditor also learned from the interview that access reports and logs exist within the card access software with no review occurring. However, the IT Manager does audit the key box access log on a weekly basis.

MICS REFERENCE: _____

FINDING:

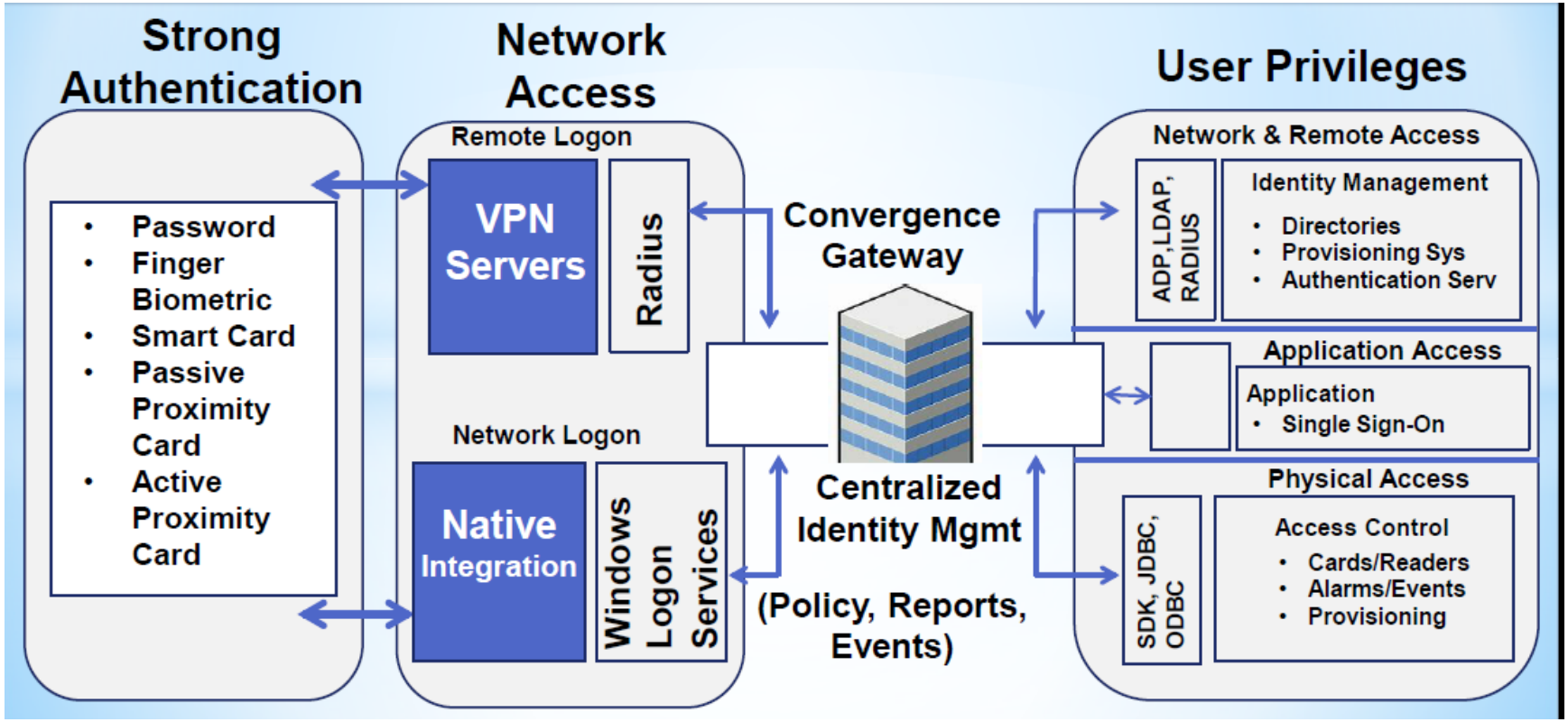
_____
_____
_____
_____
_____
_____
_____
_____

RECOMMENDATION:

_____
_____
_____
_____
_____
_____

Handout #4

Logical Security



HANDOUT #5

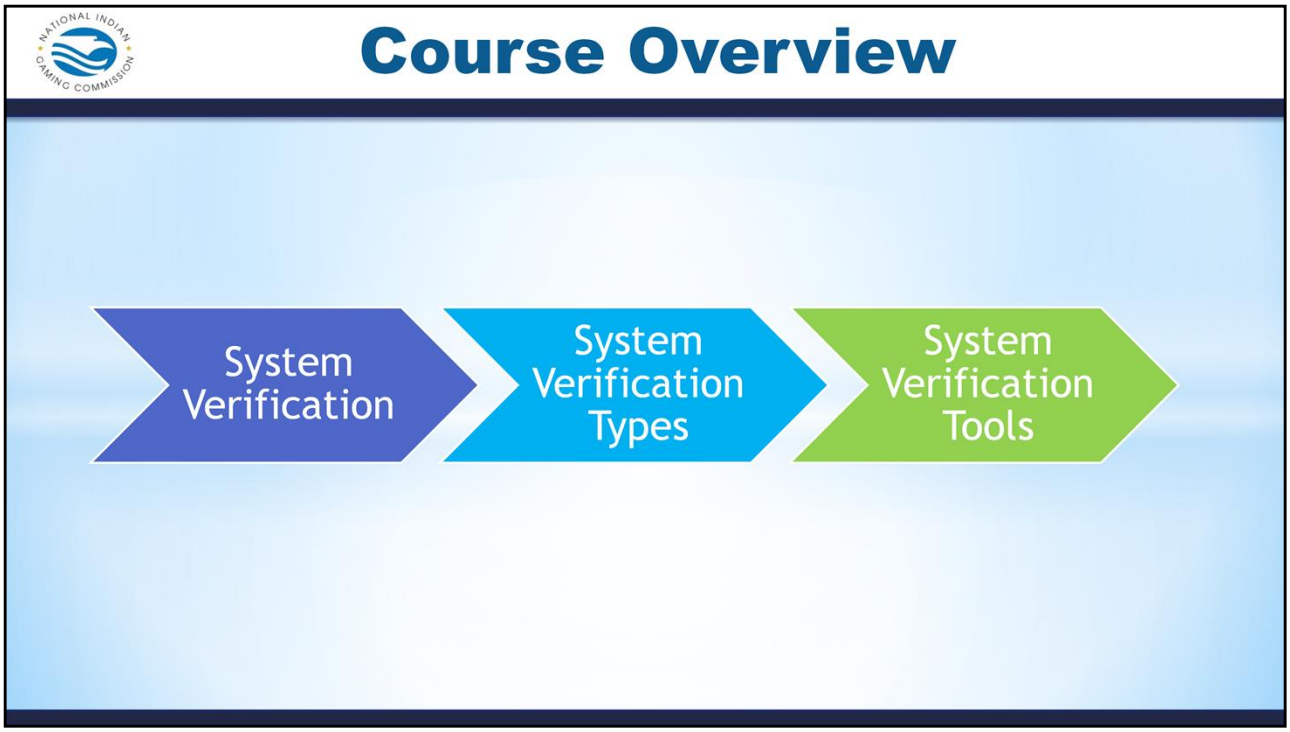
Monthly Logon/Logoff Report								
Login	Logout	Group	Computer	Port	Remote IP	Username	Logon Type	Duration
Wed 2017-24-01 03:23:43PM	Wed 2017-24-01 04:25:44PM	Casino Name	DB Server	4025	10.70.158.129	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Thur 2017-24-01 03:23:43PM	Thur 2017-24-01 04:25:44PM	Casino Name	DB Server	4076	10.70.158.145	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s
Tue 2017-24-01 03:23:43PM	Tue 2017-24-01 04:25:44PM	Casino Name	DB Server	5284	10.70.158.121	Vendor\Name of individual performing work	Terminal Services	1h 2m 41s

IT-112 System Verifications & Authentication

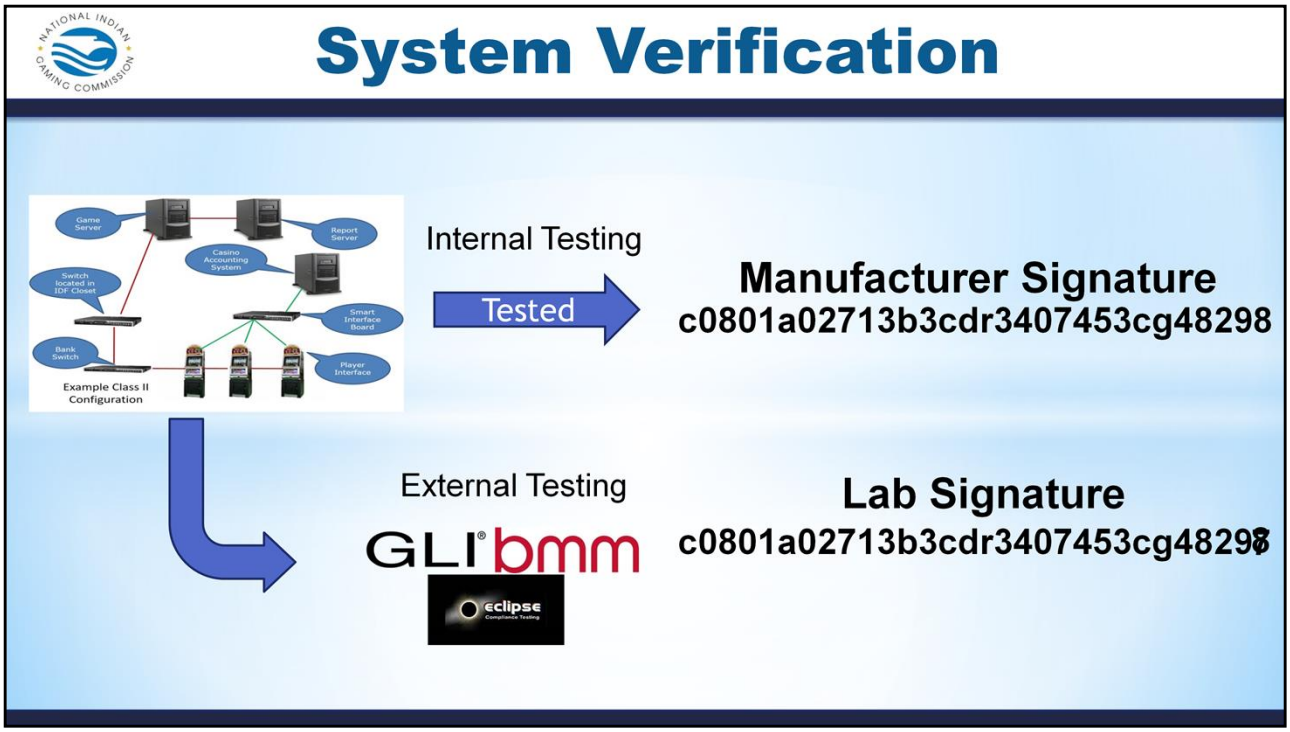
IT-112 System Verifications & Authentication

Information Technology Division

KEY POINTS

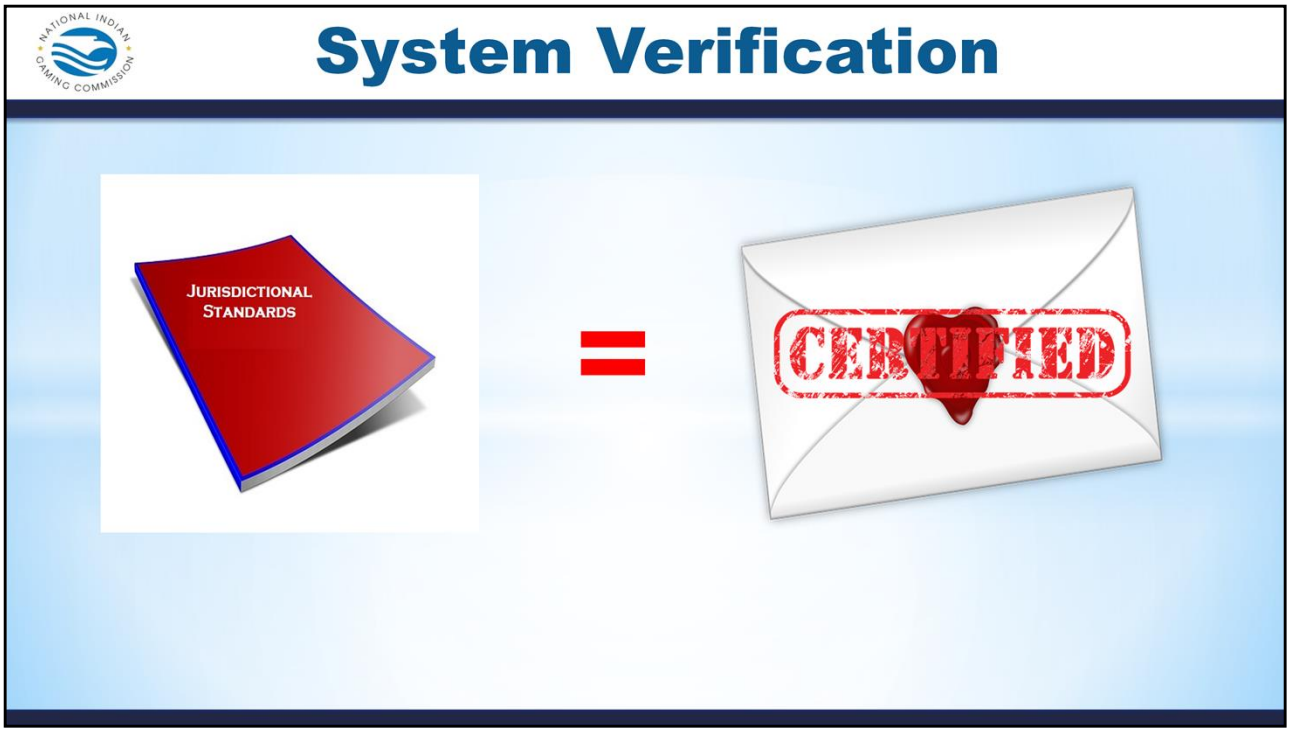

Course Overview
System Verification
System Verification Types
System Verification Tools

KEY POINTS



KEY POINTS

- The system or game is tested and assigned a signature before and after the testing is done by your ITL.
- Their may be 2-3 or more iterations of a single piece of software from a single submission.
- Insures the software tested at the ITL is what is present on the floor of my operation.
- Consists of verifying the controlled files found in system will match those that have been through the Independent Testing Lab

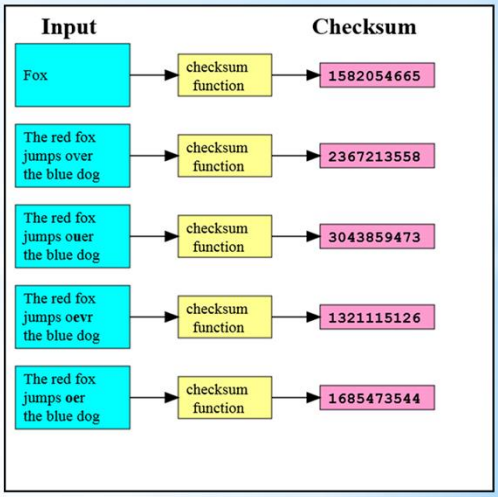


KEY POINTS

- Comply with your jurisdictional standards
- Using the tools to create the original signature that is present on the Certification Letter from the ITL
- The signature should match the Certification letter from the ITL

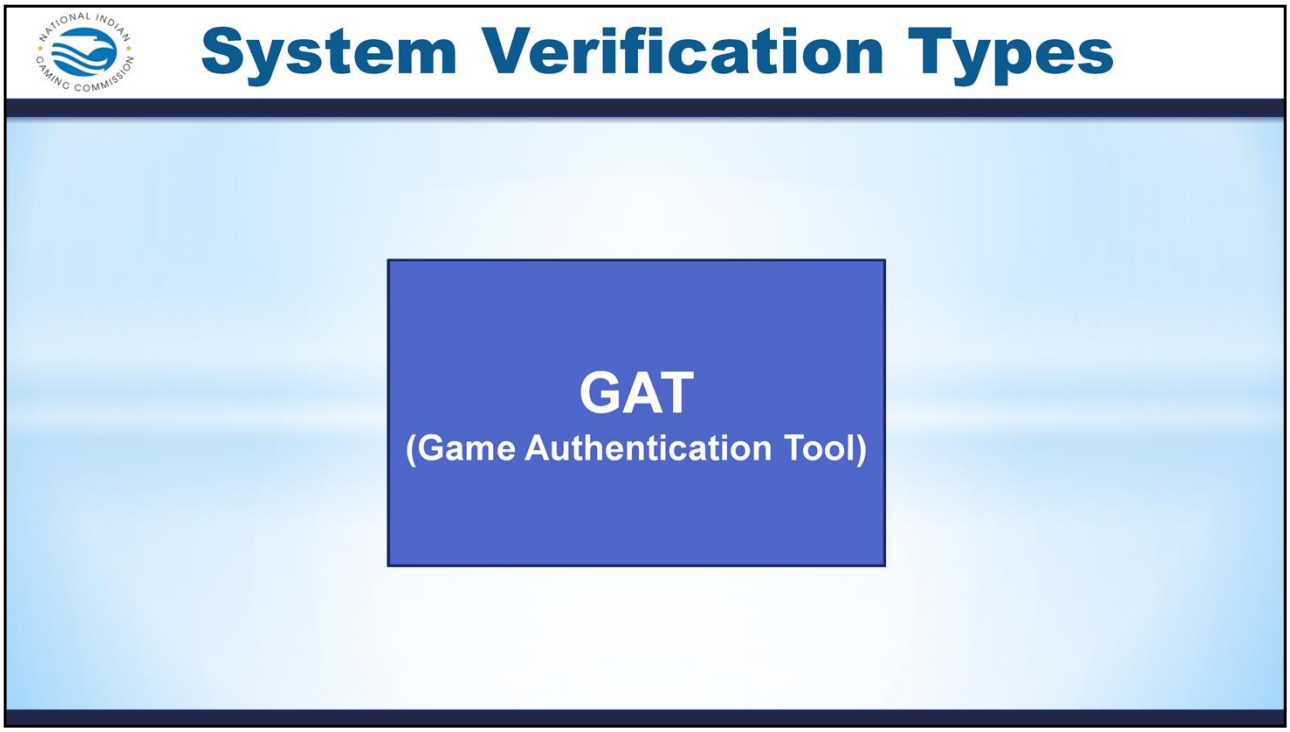
System Verification

- SHA-1
- SHA-256
- SHA-512
- MD5
- CRC-16 cyclic redundancy check
- CRC-32 cyclic redundancy check
- Checksum
- GAT



KEY POINTS

A wide variety of checksum algorithms exist each with it's own design goals and limitations.



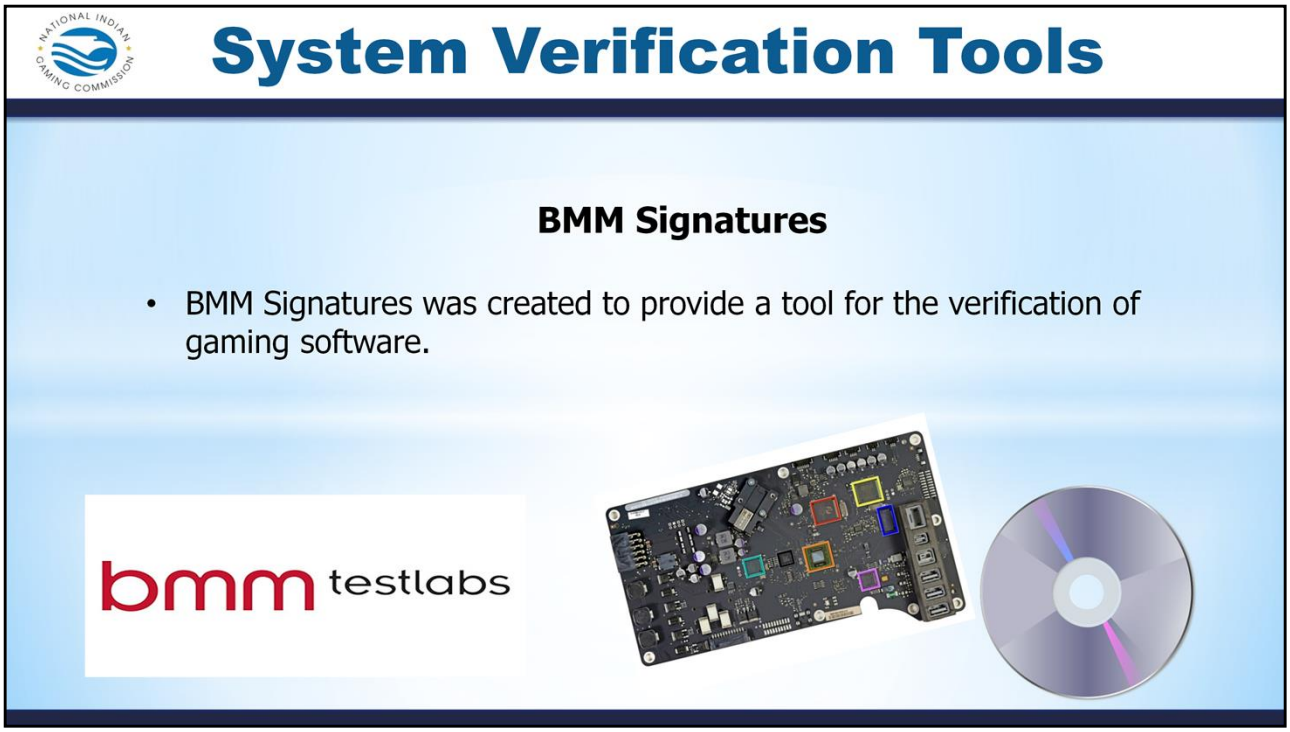
KEY POINTS

GSA GAT – Newer. Industry standard. Not widely adopted, yet. Allows for remotely verifying EGMs.

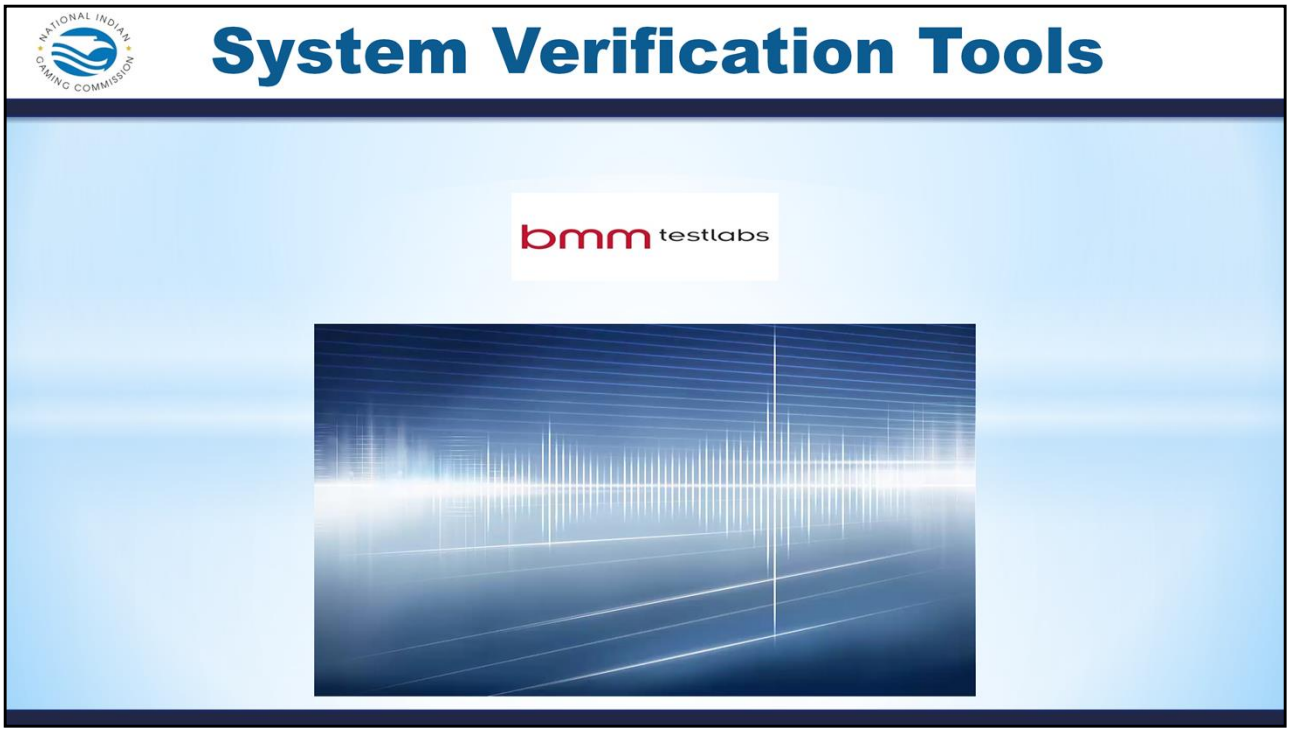

System Verification Tools
Verify+ by Kobetron is an application developed by Gaming Laboratories International, LLC. (GLI) that will generate various signatures on files, folders, DVD, CD and Compact Flash media.
GAMING LABORATORIES INTERNATIONAL®
VERIFY+

KEY POINTS

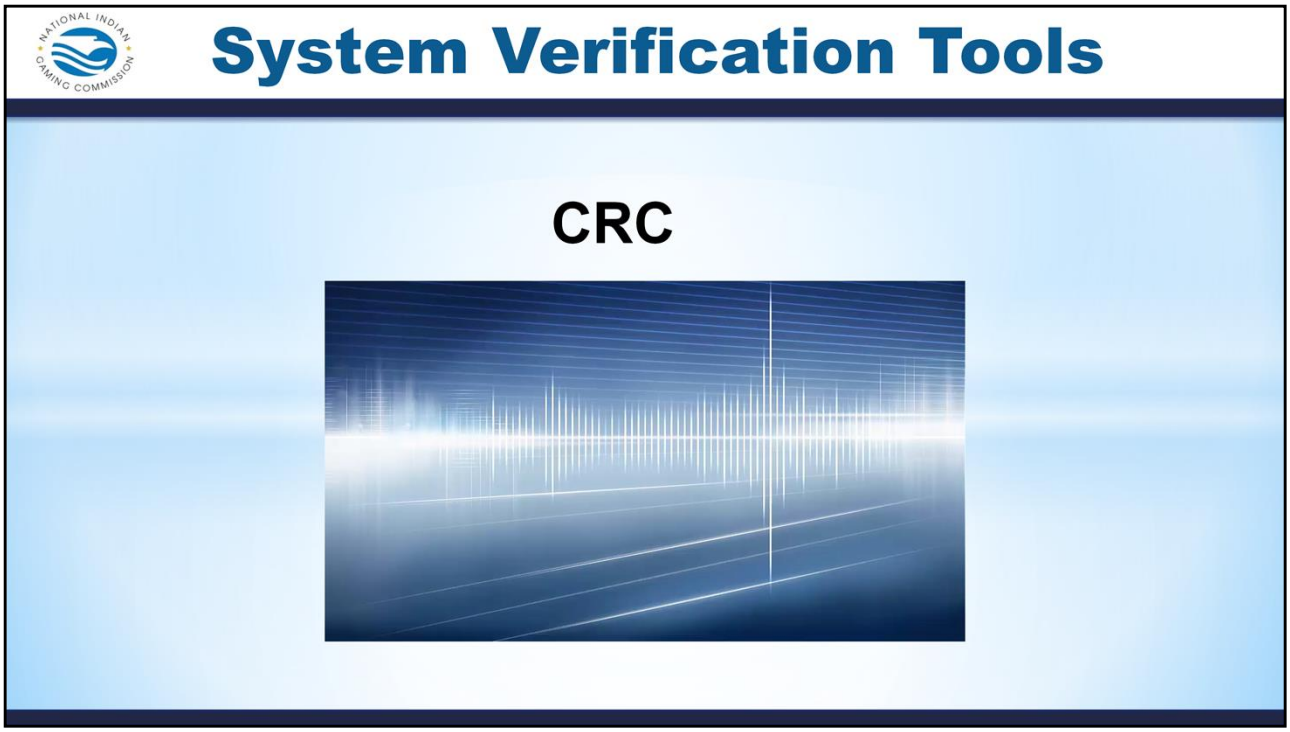
KEY POINTS


System Verification Tools
BMM Signatures
• BMM Signatures was created to provide a tool for the verification of gaming software.
bmm testlabs

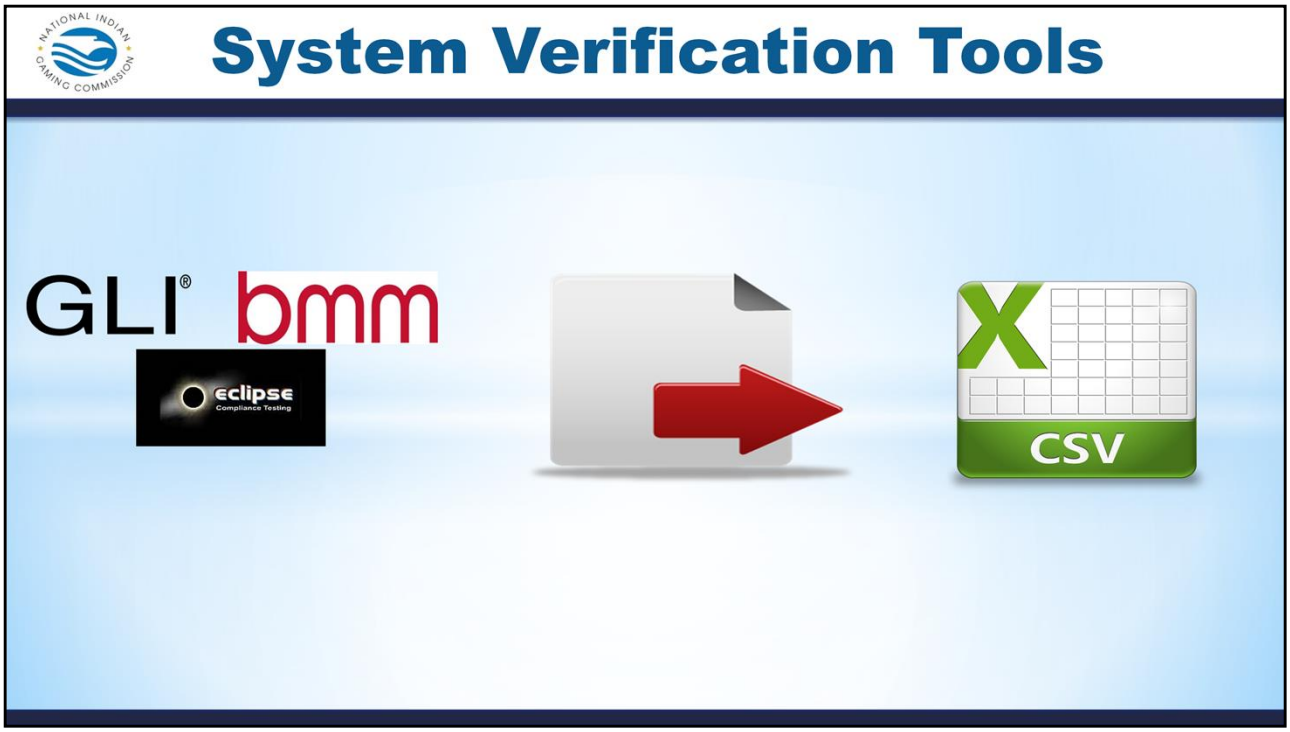
KEY POINTS



KEY POINTS

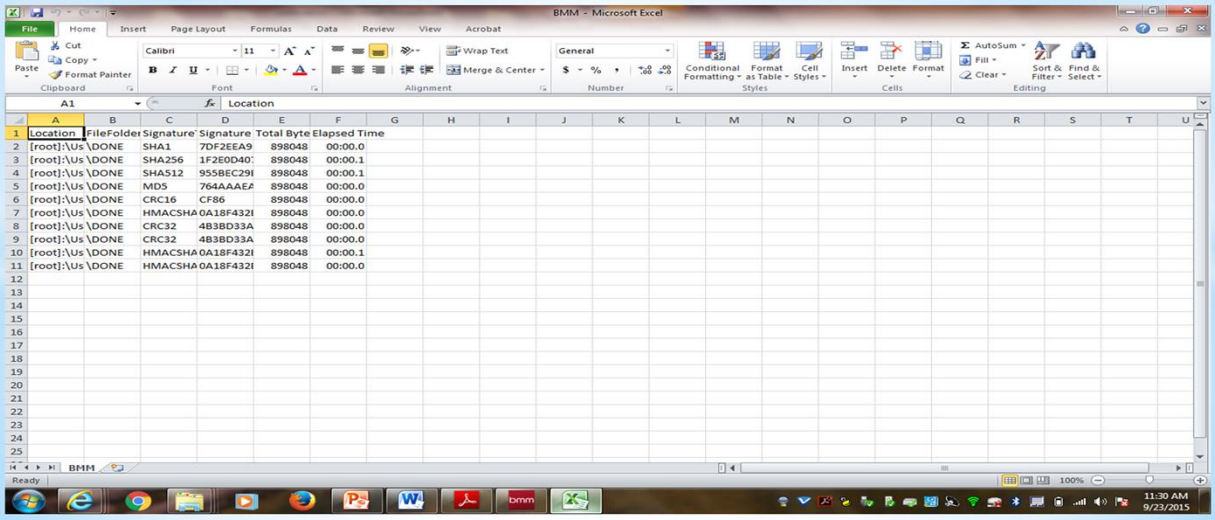


KEY POINTS

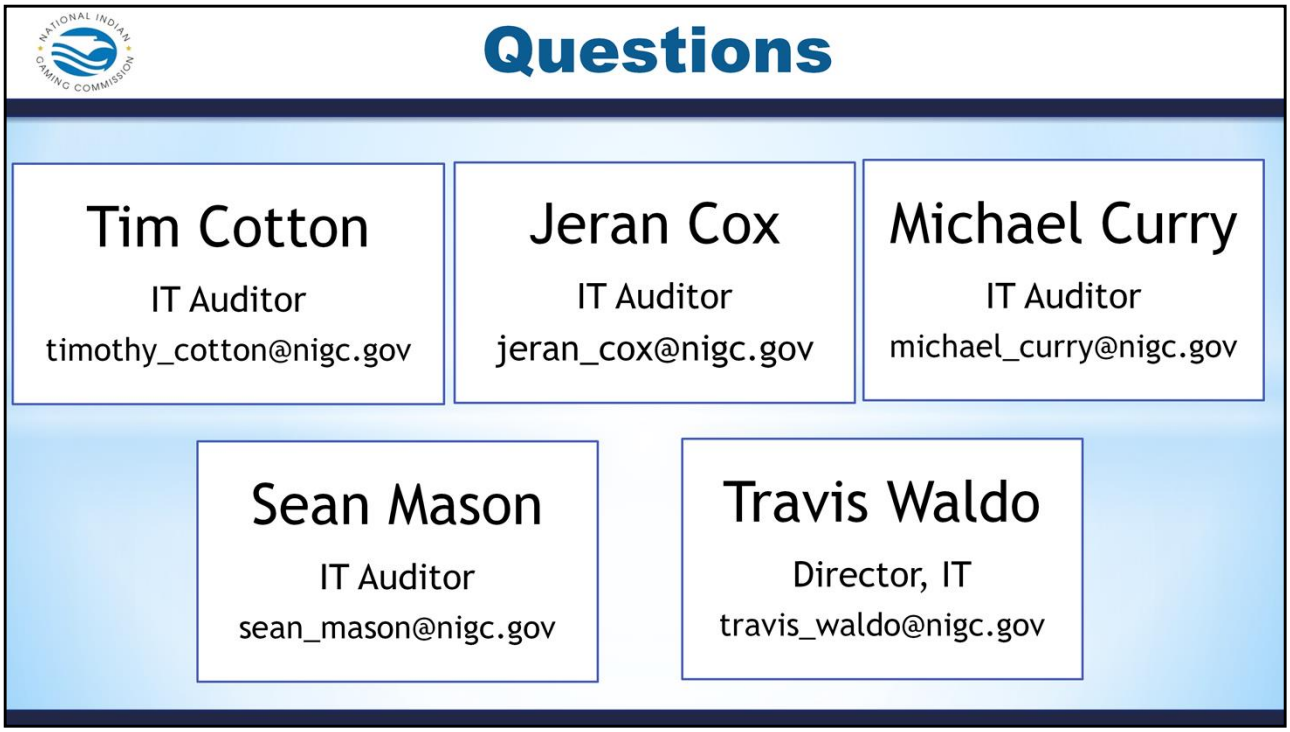

System Verification Tools
GLI
bmm
eclipse
Compliance Testing
CSV

KEY POINTS

System Verification Output



KEY POINTS


Questions
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov
Jeran Cox
IT Auditor
jeran_cox@nigc.gov
Michael Curry
IT Auditor
michael_curry@nigc.gov
Sean Mason
IT Auditor
sean_mason@nigc.gov
Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS


Course Evaluation
• Provide an honest assessment of your experience
• Written suggestions and comments are greatly appreciated and allow us to improve your experience

KEY POINTS

KEY POINTS

Poll Title: Course Eval IT-111 System Verification

https://www.polleverywhere.com/surveys/j0KEUu0ea

THIS REPORT CONTAINS A SPECIAL NOTE (denoted by " LOOK ")

Date of Report: *insert date*

The Certification report will be issued to each TGRA

Issued To: Tribal Gaming Regulatory Authority
123 Any Street
Any Town, USA 12345

Issued By: Gaming Laboratories World Headquarters
Christine M. Gallo
Vice President of Technical Compliance and Quality Assurance
600 Airport Road, Lakewood, NJ 08701
(732) 942-3999
www.gaminglabs.com

Tested By: Gaming Laboratories World Headquarters
600 Airport Road, Lakewood, NJ 08701

Certification of: **One New ACME Bingo Gaming Company Mega Bingo System version 1.1**

This describes the product(s) submitted by the manufacturer for testing

GLI File Numbers: SY-xxx-xxx-xx-xx

Standards Tested Against and the Test Results:

All applicable technical standards of the TGRA will be noted in this section

Standards Tested Against	Test Results
National Indian Gaming Commission (NIGC) Minimum Technical Standards for Electronic, Computer or Other Technologic Aids Used in the Play of Bingo	Pass or Fail
Any Additional Standards the TGRA has adopted the Class II Minimum Technical Standards	Pass or Fail

SYSTEM

System Software Descriptions:

- **This section will describe the Bingo Gaming System including the roles and responsibilities**
- **All of the files that affect the play of the game, accounting or game functionality will be identified in this section along with a description the file is responsible for**
- **This section can be quite extensive as it covers all .exe, .dll, .sql and other files that affect the integrity, accounting or play of the game**
- **All of the identified files will be version and signature controlled and will be contained within the certification letter**

EXAMPLE

MBS.exe

The Mega Bingo System (MBS) is the application within the Bingo Gaming System that is responsible for the play of electronic bingo and all related functions such as the communication between the electronic player interface and the MBS. This application also manages the financial results from the bingo game including any progressive, bonusing or mystery jackpot functionality.

All of the files called out in the description section will be noted here by version and applicable signatures

System Software Being Certified:

List overall system name and version

File Name	Version	Type	GLI Verify® CDCK Signature	GLI Verify® SHA-1 Signature
MBS.exe	1.1	CL2	ABCD	ABCD123456789DCBA987654321ABCD1234567

System Software Modifications:
Any modifications from a previous GLI certification report would be noted in this section

System Software Notes:
Any additional notes that would be important to the TGRA regarding the software would be noted here

EXAMPLE

Testing has been done only on Class II Bingo. Any other capabilities are not tested or approved.

Please note the items certified in this report were tested as per the manufacturer's intended specifications for the Class II market. It may be possible to alter configurations, which may result in the gaming system component(s) becoming non-compliant.

Terms and Conditions:

This Report is issued solely for the benefit of the Client for use only for and limited to the specific jurisdiction or standards referenced in the Report. This Report may not be relied upon for any reason by any person or entity other than the Client including, but not necessarily limited to, the manufacturer or developer of the items, a non-GLI Laboratory, or a Regulator not named in the Report ("a Third Party").

Any report produced by GLI is proprietary to GLI and the Client, because it contains confidential information of commercial value, the exposure of which to third parties could adversely affect both GLI and the Client. Accordingly, such confidential information is supplied in confidence, on the strict condition that no part of it will be reprinted or reproduced or transmitted to any parties external to the original contract without the prior written approval of the Parties. In particular, it will not be exposed to any person or organization which may be in competition with any of the Parties without the prior written approval of that Party. The testing performed by GLI is proprietary to GLI and/or various regulators. No third party may use, rely or refer to a GLI evaluation report, test report, certification document or test results without written permission of GLI and the respective regulator. Notwithstanding the above, the Parties may disclose confidential information if required to do so by regulatory agencies, pursuant to the laws and regulations of an applicable jurisdiction or by an order of a properly designated Court of Law in a relevant jurisdiction. However, in either case the Parties agree to immediately notify the other party of such a request.

Notwithstanding the above, any regulator may reprint, reproduce and transmit any document or information to any party that the regulator, in their sole discretion, deems appropriate.

The certification established by this Report applies exclusively to tests conducted using current and retrospective methods developed by **Gaming Laboratories International, LLC** (GLI) on the specific items submitted by the Manufacturer identified by the words "**Certification of:**" on the first page of this Report. It is the responsibility of the manufacturer and/or developer of the items submitted to apply for, obtain and maintain all necessary gaming licensure in each jurisdiction in which they do business, including state and tribal jurisdictions, where applicable. The Electrostatic Discharge Testing performed by GLI is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of Electronic Gaming Devices. During the course of testing, GLI checks for marks, symbols or documents indicating that a device has undergone product safety or RoHS compliance testing, if required. GLI also performs a cursory review of information accompanying the items submitted, where possible and when provided, for evidence that the items have undergone compliance testing for Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations, Electrostatic Immunity, Electro Magnetic Compatibility and Environmental conditions. Compliance with any such regulations related to the aforementioned testing is the sole responsibility of the manufacturer and/or developer of the items submitted; GLI accepts no responsibility, makes no representations and disclaims any liability with respect to all such non-gaming testing. The test methods used, excluded tests, and actual data showing the test results are available to the Recipient upon written request.

All items identified in the "Certification of:" section on the first page of the report are considered certified as of the date shown in the "Date of Report:" section on the first page of the original GLI issued Report. All of the items are certified for use until such time notification is sent indicating that an item is no longer permitted to be used within the jurisdiction specified. Additional information regarding the validity of this certification can also be obtained via GLIAccess and/or the Evaluation and Certification Guide, which is available on the gaminglabs.com website. Use of the Certified Mark represents the users agreement to permit, allow and accommodate authorized representatives of GLI to perform a surveillance audit of the use of the Mark and to permit an authorized representative of the American Association of Laboratory Accreditation (A2LA) to perform a surveillance audit, at their discretion and at their expense, to confirm that the use of the Mark in no way implies that A2LA endorses or certifies any of the Marks, services or processes of the company, group or organization requesting the use of the GLI Certified Mark.

GLI WARRANTS TO THE RECIPIENT THAT ALL SERVICES PROVIDED BY GLI HEREUNDER HAVE BEEN PERFORMED IN ACCORDANCE WITH ESTABLISHED AND RECOGNIZED TESTING PROCEDURES AND WITH REASONABLE CARE IN ACCORDANCE WITH APPLICABLE LAWS. GLI DOES NOT MAKE, AND EXPRESSLY DISCLAIMS, ALL OTHER WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SUITABILITY OR FITNESS FOR A PARTICULAR PURPOSE. GLI DOES NOT WARRANTY ANY TESTING OR RESULTS FROM A NON-GLI LABORATORY. WITHOUT LIMITING ANY OF THE FOREGOING, UNDER NO CIRCUMSTANCES SHOULD THE CERTIFICATION ESTABLISHED BY THIS REPORT BE CONSTRUED TO IMPLY ANY ENDORSEMENT OR WARRANTY REGARDING THE FUNCTIONALITY, QUALITY OR PERFORMANCE OF THE SUBJECT HARDWARE OR SOFTWARE, AND NO PERSON OR PARTY SHALL STATE OR IMPLY ANYTHING TO THE CONTRARY. THE LIABILITY AND OBLIGATIONS OF GLI HEREUNDER, AND THE REMEDY OF THE RECIPIENT, UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO, AT GLI'S OPTION, REPLACEMENT OF THE SERVICES PROVIDED OR THE REFUND BY GLI OF ANY MONIES RECEIVED BY IT FOR THE SERVICES PROVIDED. IN NO EVENT SHALL GLI BE RESPONSIBLE TO THE RECIPIENT OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR REVENUE, BUSINESS INTERRUPTION, OR PUNITIVE DAMAGES, EVEN IF GLI HAD BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES AND WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW OR OTHERWISE. ALL RIGHTS AND REMEDIES OF THIRD PARTIES RELATING TO PRODUCTS AND SERVICES THAT ARE THE SUBJECT OF THE CERTIFICATION ESTABLISHED BY THIS REPORT SHALL BE THE EXCLUSIVE RESPONSIBILITY OF THE RECIPIENT AND GLI EXPRESSLY DISCLAIMS ANY LIABILITY WHATSOEVER IN CONNECTION WITH SUCH THIRD PARTY RIGHTS AND REMEDIES. GLI AND THE RECIPIENT ACKNOWLEDGE AND AGREE THAT THE SERVICES PROVIDED BY GLI HEREUNDER COULD NOT BE RENDERED BY GLI UNDER THE TERMS PROVIDED HEREIN WITHOUT AN INCREASE IN COST IF GLI WAS REQUIRED TO PROVIDE ANY WARRANTIES IN ADDITION TO, OR IN LIEU OF, OR WAS REQUIRED TO ASSUME ANY LIABILITY IN EXCESS OF, THE FOREGOING.

If you should have any questions regarding this information, please feel free to contact our office.

Sincerely,
GAMING LABORATORIES INTERNATIONAL, LLC

Christine M. Gallo
Vice President of Technical Compliance and Quality Assurance

c: *manufacture contact, manufacture name*

BMM COMPLIANCE TEST REPORT

Report Issue Date: 13th December, 2017

Issued To: Tribal Gaming Regulatory Authorities

Issued to all tribes

Issued By:
BMM Testlabs
Travis Foley, Executive Vice President, Operations
815 Pilot Road, Suite G, Las Vegas, NV 89119
(702) 407 2420, www.bmm.com

Compliance Tested By:
BMM Testlabs
815 Pilot Road, Suite G
Las Vegas, NV 89119

Manufacturer:
ABC Manufacturer, Inc.
123 Sample Drive
Las Vegas, NV 89123

Manufacturer & Address

Compliance Review for:

Gaming System: Class II Bingo System v1.06

Gaming System Component: Class II Game Theme v1.44

This describes the items being reviewed within this report. This report shows a system and theme.

Reference Numbers:

BMM: MFG.1001

Report Number: MFG10011_TGRA

1. STANDARDS TESTED TO/RESULT

Technical Standards used for Compliance Evaluation:	Test Result	
	Pass	Fail
NIGC 25 CFR Part 547: Minimum Technical Standards for Class II Gaming Systems and Equipment, effective October 22, 2012	☑	❑
NIGC 25 CFR Part 543: Minimum Internal Control Standards, effective October 22, 2012	☑	❑

Technical standards used for the review.

And the characteristics of each item.

2. GAMING SYSTEM COMPLIANCE DETAILS

2.1. Gaming System Characteristics:

The Class II Bingo System v1.06 is the main software used to control the main functions of the gaming platform. The module can be used for multiple games and is responsible for but not limited to the following functions:

- Game accounting
- Service menu and settings
- SAS communications protocol
- Peripherals communications
- File signature verification
- Control program authentication
- Manages communications with the Central Ball Call Server.

2.2. Gaming System File Details:

The following table details the relevant information for the Class II Bingo System v1.06 that has been verified as compliant to the aforementioned Technical Standards:

On screen signatures

Product ID	Product Version	Product Type	System name	Signature	Signature Type
Class II Bingo System	1.06	Gaming System	CLASS2_SYSTEM	411D2D98195B3E133589 DE81C55AE498AEDC42F8	SHA-1
Location: Attendant Menu -> Diagnostics-> Versions Validation Program Used: On-Screen Hash					

Note: *This signature is generated by the manufacturer of the gaming device and not by BMM Testlabs.*

Note*: Refer to Section 2.4 for verification tools used.*

Signature Information

2.3. Additional Class II Bingo System v1.06 Program Notes:

- **Compatible Electronic Player Interface**: ABC model number CAB0003

  The Class II Bingo System v1.06 detailed within this report is compatible with ABC gaming Electronic Player Interface model number CAB0003
- Appendix 1 gives the details of the supported game and main functionality.
- Appendix 2 gives the details of the supported game and system SAS functionality.

2.4. Software Signature Verification Information:

Signature Verification Application:

(1) Signature verification procedures may require administrator rights access.

Signature Verification Procedure:

Generating the Game Generated Hash:

1. Open the Main door.
2. Turn the operator key to access the menu.
3. Using the "Previous" or "Next" buttons select the "Diagnostics" option from the menu.
4. Select "Version" from the menu.
5. The program hashes will be displayed on screen.
6. Verify that the signatures obtained match those listed in Section 2.2 of this report.

3. GAMING SYSTEM COMPONENT COMPLIANCE DETAILS

3.1 Gaming System Component Characteristics:

Class II Game Theme v1.44 is an Electronic Real Time Bingo game that uses the Bingo Cash Hits 40 Lines v1.00 as math asset. The math asset contains the pay-table files for the Class II Game Theme game. The characteristics of the game are given below:

- This game theme is an electronic video bingo game with a visual aid. The visual aid is for entertainment purposes only.
- This game requires a minimum of two (2) players to initiate play which must be configured by the operator from the server. The game does not initiate until the required number of players are participating.
- A bingo card is provided by the game with spaces arranged in five (5) columns and five (5) rows, with numbers assigned to each space. Bingo card selections can be changed prior to game initiation by touching the bingo card displayed on the entertaining display. No free spots are available on the bingo card.
- For a win to occur, the bingo card pattern has to match a predetermined bingo winning pattern. Each predetermined bingo pattern has its own payout amount. The winning patterns and corresponding win amount are available to the patron in the help screens prior to the commencement of each game.

- The highest bingo pattern is awarded when multiple winning combinations are marked on the bingo card.
- The bingo numbers are randomly drawn by an electronic Random Number Generator (RNG) located on the server. The RNG outcome represents the ball draw for the game.
- All players will receive 75 bingo balls.
- The Bingo game outcome is determined by group of patterns arranged from pattern 1 to 1615. Outcome is determined by the first completed pattern group.
- Determination of the Bingo award is in ascending order.
- All pattern groups are marked using the same bingo card. Each pattern group may contain up to five (5) bingo patterns.
- Main game is based on bingo. The Bonus features are not based on bingo, but the feature is triggered by certain bingo combinations.

The following details the visual aid of the bingo game Class II Game Theme v1.44:

- This game has an entertaining display represented by five (5) visual aid reels and 40 graphical lines.
- All win amounts displayed by the entertaining display are determined from the bingo game winning patterns.
- Winning patterns are displayed on the entertaining display as winning combinations that start from leftmost visual aid reel to right only and are represented as line pays, scatter pays, or in a bonus game.

Entertaining Display

- Two (2) “$” visual aid symbols appear on reels 2 and 5 will trigger the Bonus entertaining display and award 10 free spins entertaining display.
- Free Spins entertaining display contains different reels strips with “blanks” and “$” visual aid symbols.
- The oversized “$” visual aid symbol is two (2) symbols tall and if half of the “$” visual aid symbol is visible, prizes are still awarded.
- Prizes are multiplied by total bet. Every “$” visual aid symbol appearing during the Cash Hit entertaining display Feature pays.
- Progressive jackpots cannot be triggered during this entertaining display. Bonus entertaining display cannot be retriggered.

Progressive Jackpot

- Progressive jackpots are available on the first four (4) visual aid entertaining display pay-lines only.
- Progressive jackpot is available only at the max bet.
  - "$" and "777" visual aid symbols appearing on reels 2,3,4,5 will trigger Level 1 Progressive.
  - "$" and "77" visual aid symbols appearing on reels 2, 3, 4 will trigger Level 2 Progressive.
  - "$" and "7" visual aid symbols appearing on reels 2, 3 will trigger Level 3 Progressive.

PROGRESSIVE FEATURE:

Three (3) Levels Supported

3.2 Gaming System Component File Details:

The following table details the relevant information for Class II Game Theme v1.44 that has been verified as compliant to the aforementioned Technical Standards:

Product ID	Product Version	Product Type	Filename	Signature	Signature Type
Class II Game Theme	1.44	Gaming System Component	abc.rom	7C35626A53D85EC1A9B986C3FEE0404DBF1B1D37	SHA-1
Location: Game SATADOM Validation Program Used: BMM Signatures v2.0.1					

***Note**: Refer to Section 3.5 for verification tools used.*

On Screen Signatures

The following are game generated hash values and are given for field verification purposes only.

7 Dollars Classic Edition v1.44

Product ID	Product Version	Product Type	Program Name	Signature	Signature Type
Class II Game Theme	1.44	Program	ABC_CLASS2_SYSTEM Theme	AB7D0C7E322D3021D4B71B5A4C9C2CF2	MD-5
Location: Attendant Menu -> Diagnostics-> Versions Validation Program Used: On-Screen Hash					

***Note:** This signature is generated by the manufacturer of the gaming device and not by BMM Testlabs.*

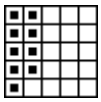
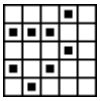
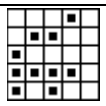
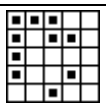
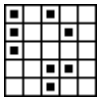
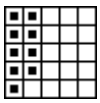
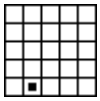
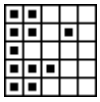
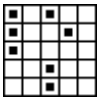
***Note**: Refer to Section 3.5 for verification tools used.*

3.3 Additional Gaming System Component Details:

Mathematical Fairness Details:

The following tables detail the fairness standards outlined in §547.5(c):

Top Prize Details for Advertised Prize:

Variation	Top Prize	Top Prize Odds	Top Prize Description
All Non Max Bet	5,870 Credits	1 in 55,344,776	Hit all 5 bingo patterns in below group within corresponding numbers of balls, without hitting any prior group in the pattern groups' priority list. 25  51  74  75  73 
All Max Bet	10,800 Credits	1 in 53,005,241	Hit all 4 bingo patterns in below group within corresponding numbers of balls, without hitting any prior group in the pattern groups' priority list. 25  3  45  55 

Note: For max bet 200 credits, actual top award will be the published amount plus progressive increment.

Progressive Capability Details:

Game Component	Progressive Capability	Progressive Levels
Class II Game Theme	Yes	Three (3)

Denomination and Credit Values:

Game	Variation	Denominations
Class II Game Theme	ALL	$0.01, $0.02, $0.05, $0.10, $0.20, $0.25, $0.50, $1.00, $2.00, $5.00, $10.00

Max Bet Details:

Game	Max Bet
Class II Game Theme	200 Credits

3.4 Additional Program Notes:

- **Compatible Gaming System:** Class II Bingo server 1.02 or higher.

  The Gaming system component detailed in this report is anticipated to be compatible with any subsequent released versions of Class II Bingo server 1.02 or higher.
- **Compatible Class II System: Class II Bingo System v1.06**

  The Gaming system component detailed in this report is compatible with Class II Bingo System v1.06
- **Compatible Electronic Player Interface**: ABC model number CAB0003
- The Class II Bingo System v1.06 detailed within this report is compatible with ABC gaming Electronic Player Interface model number CAB0003
- **Compatible Backend Systems:** Bally ACSC, Bally- SDS, IGT advantage, Aristocrat OASIS, KCMS

  The Class II Game Theme detailed in this report was tested for accounting reporting only with the subsequent released versions of Bally ACSC, Bally- SDS, IGT advantage, Aristocrat OASIS, and KCMS.
- The Gaming System Class II Bingo System v1.06 and Gaming System Component Class II Game Theme v1.44 are combined together in the file abc.rom on the SATADOM.
- Appendix 3 gives the details of the Payout Percentage (RTP) information for the Gaming System Component.

Additional notes, be sure to read this section in live reports.

3.5 Software Signature Verification Information:

Signature Verification Application:

(1) The SHA-1 signatures were calculated and verified using the BMM Signatures proprietary verification tool, which has been calibrated in accordance with ISO/IEC 17025 sections 5.5.2, 5.5.a, 5.5.c, and 5.5.8; as well as ISO/IEC 17020 sections 9.4, 9.6.b, 9.13.a, and 9.15.

(2) Where requested, BMM will supply the regulator/operator with BMM's proprietary verification tool "BMM Signatures" for verifying the SHA-1 details above. A user manual will also be supplied.

(3) Signature verification procedures may require administrator rights access.

Signature Verification Procedure:

1. Install BMM Signatures v2.0.1 and double click on the "BMM Signatures 2.0" icon.
2. The BMM Signatures program will open.
3. Insert the game USB into the laptop that will run BMM Signature.

Signature Verification for Individual Files

1. Select the "Files and Folders" tab.
2. Select the "Browse Files" tab.
3. Navigate to the SATADOM and locate the file listed in section 3.2 of this report.
4. Click the desired algorithm to use (e.g. SHA1). When the program is completed, the signatures will be displayed in the Output window.
5. Verify that the software file signature obtained matches the signature listed in section 3.2 of this report.

High-level steps to verify the software. Detailed steps would be found in a field verification manual for the platform.

Generating the Game Generated Hash:

7. Open the Main door.
8. Turn the operator key to access the menu.
9. Using the "Previous" or "Next" buttons select the "Diagnostics" option from the menu.
10. Select "Version" from the menu.
11. The program hashes will be displayed on screen.
12. Verify that the signatures obtained match those listed in Section 3.2 of this report.

4. TERMS AND CONDITIONS

BMM Testlabs ("BMM") has conducted a level of testing of the gaming product which has historically been adequate for a submission of this type. However, inherent in testing in a laboratory environment are the unavoidable limitations of not being able to verify the effects of all possible configurations and environments that occur in actual gaming venues.

This compliance report is for use by the client for the jurisdiction ("Jurisdiction") referenced in the report (the "Report") and only verifies, as of the date stated, the gaming product described in the Report subject to any conditions or limitations set forth therein.

The manufacturer named in the Report is solely responsible for possession of the appropriate license to sell, lease, service, or provide gaming supplies or gaming-related services in the Jurisdiction and for compliance with the ongoing requirements of the Jurisdiction. It is the responsibility of the manufacturer and operators to ensure that the gaming product detailed in this Report is installed, maintained and operated correctly without defects and safely in accordance with requirements of the Jurisdiction.

The Report and testing performed by BMM is proprietary to BMM. This Report is issued solely for the benefit of the client and shall not be reproduced, reprinted, or transmitted in whole or in part to any party not named in the Report without the written approval of BMM, other than by a regulator of the Jurisdiction. No third party may use, rely, or refer to the Report, its contents, or any related documents, without written permission of BMM. If BMM grants consent, BMM will send this Report via email as directed. BMM takes precautionary measures to secure the "PDF" document, but BMM does not send the email via any encrypted methodology.

The undersigned certifies under penalty of perjury that the compliance testing of the gaming product detailed in this Report and any accompanying documents was conducted in accordance with the requirements of the Jurisdiction and that the gaming product meets the requirements of its laws and the regulations adopted thereunder, and all published technical standards, control standards, control procedures, policies, industry notices and similar requirements implemented or issued by the Jurisdiction to the best of BMM's knowledge and belief.

Notwithstanding the above, any regulator may reprint, reproduce and transmit any document or information to any party that the regulator, in their sole discretion, deems appropriate.

BMM DOES NOT MAKE, AND EXPRESSLY DISCLAIMS, ALL OTHER WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SUITABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE LIABILITY AND OBLIGATIONS OF BMM HEREUNDER, AND THE REMEDY OF THE RECIPIENT, UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO, AT BMM'S OPTION, REPLACEMENT OF THE SERVICES PROVIDED OR THE REFUND BY BMM OF ANY MONIES RECEIVED BY IT FOR THE SERVICES PROVIDED. IN NO EVENT SHALL BMM BE RESPONSIBLE TO THE CLIENT OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR REVENUE, BUSINESS INTERRUPTION, OR PUNITIVE DAMAGES, EVEN IF BMM HAD BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES.

Please feel free to contact BMM if you have any questions with regard to this Report.

Yours sincerely,

Travis Foley
Executive Vice President, Operations
BMM Testlabs

T/ vz, st, wh, bo

G/ su

Appendix 1

Gaming System Functionality

	Functionality	Supported
Payout Methods	Financial Instrument Dispenser(s) (Coins, Vouchers and Coupons, etc)	✓
Credit Input Methods	Financial Instrument Acceptor(s) (Coins, Bills, Vouchers and Coupons, etc)	✓
Features	Double Up	
	Multi-denomination Configuration (more than 1 denomination configuration option available)	✓
	Multi-denomination Game (more than 1 denomination available to be selected by the player)	✓
	Tournament game	
	Multi–Wager Configuration (more than 1 wager configuration option is available)	
	Multi–Wager Game (more than 1 wager selection option is available to the player)	
Progressive	Multi-Site	
	Linked (External)	
	Mystery (External)	
	Mystery (Internal)	
	Standalone (Internal)	✓

Note: Before any gaming system software component or equipment is installed for public use, BMM recommends that the regulator and/or operator personnel conduct communication testing with all associated devices to ensure its correct operation within the specific casino environment.

✓ = This functionality is supported.

Appendix 2

Functions of SAS supported by the Gaming System

	Description of Function	Supported	Pass	Fail
1	Communications (general polls and long polls)	✓	✓	
2	Multi Game			
3	Fund Transfers			
	Advanced Fund Transfers	✓	✓	
	Advanced Fund Transfers-Bonus Awards	✓	✓	
	*Electronic Fund Transfer (ECT-Credits)			
	*Electronic Fund Transfer (Dollars/cents)			
4	Progressives	✓	✓	
5	Tournament			
6	Real Time Event Reporting	✓	✓	
7	Bonusing (Legacy Bonusing)			
	Direct Bonus Award–Standard			
	Multiplied Jackpot Features			
8	Jackpot Handpay Reset	✓	✓	
9	Validation and Ticket Redemption			
	Standard Validation			
	Enhanced Validation	✓	✓	
	System Validation	✓	✓	
10	Multi-Denomination Extensions	✓	✓	
11	Component Authentication (i.e. SHA-1, CRC 32, KOBEI, KOBEII, MD5)			
12	SAS Version	6.02		

* Supports previous SAS versions EFT functionality.

✓ = This functionality is supported.

Appendix 3

Payout Percentage Information

Class II Game Theme v1.44:

Variation	RTP (%) Min/Max	Ball Draw Description
01	93.51/ 95.05	75 out of 75 balls
02	95.46 / 97.00	

Note: *Progressive contribution 1.54% included in the Max RTP, for max bet 200 credits only.*

IT-108 IT Vulnerabilities, Tech Exploits and Cyber Defenses

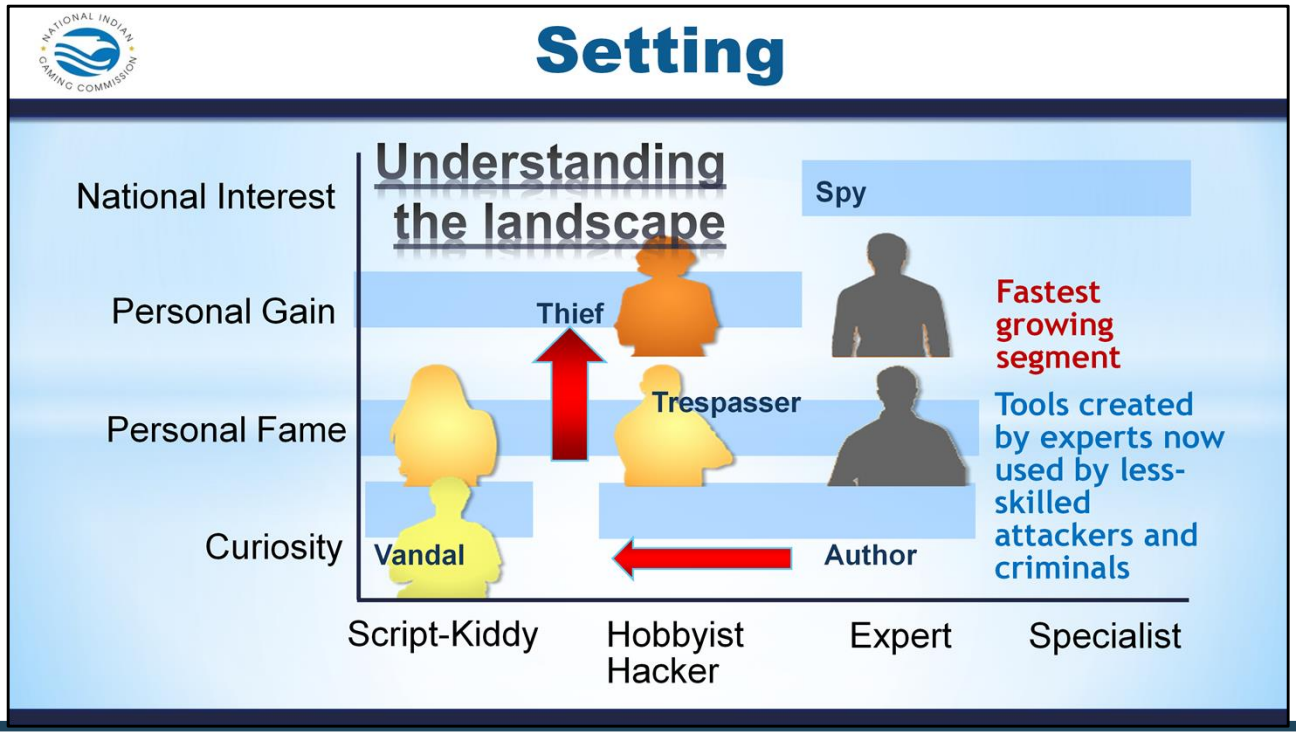
IT-108 IT Vulnerabilities, Tech Exploits, and Cyber Defenses

Information Technology Division

KEY POINTS


Overview
Defenses
Settings & Limitations
Equipment/Software
Vulnerabilities & Attacks
Human Error
New Horizons

KEY POINTS



KEY POINTS

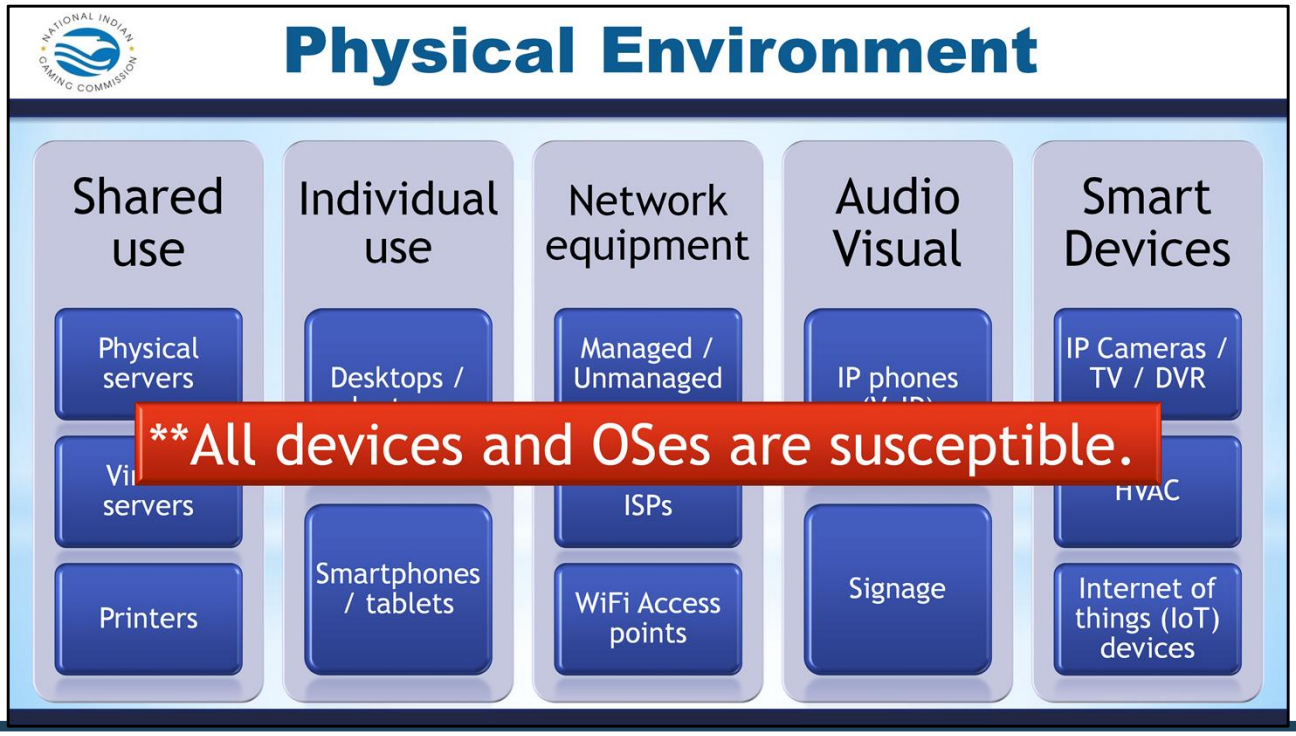
Types of attackers and reasons for attack:
Curiosity, Fame, Personal gain, National Interest
Script-Kiddy, Hobbyists, Experts, Specialist

How SAFE are you?

Entity	Year	Records	Type	Method
Yahoo	2013/14	1,200,000,000	web	hacked
Deep Root Analytics (RNC)	2017	200,000,000	web	accidentally published
Adobe Systems	2013	152,000,000	tech	hacked
Equifax	2017	143,000,000	financial	hacked
Sony	2011	77,000,000	gaming	hacked
JP Morgan Chase	2014	76,000,000	financial	hacked
Target Corporation	2014	70,000,000	retail	hacked
Commission on Elections	2016	55,000,000	government	hacked
U.S. Department of Veteran Affairs	2006	26,500,000	government, military	lost / stolen computer
Taobao	2016	20,000,000	retail	hacked
Vodafone	2013	2,000,000	telecoms	inside job

KEY POINTS

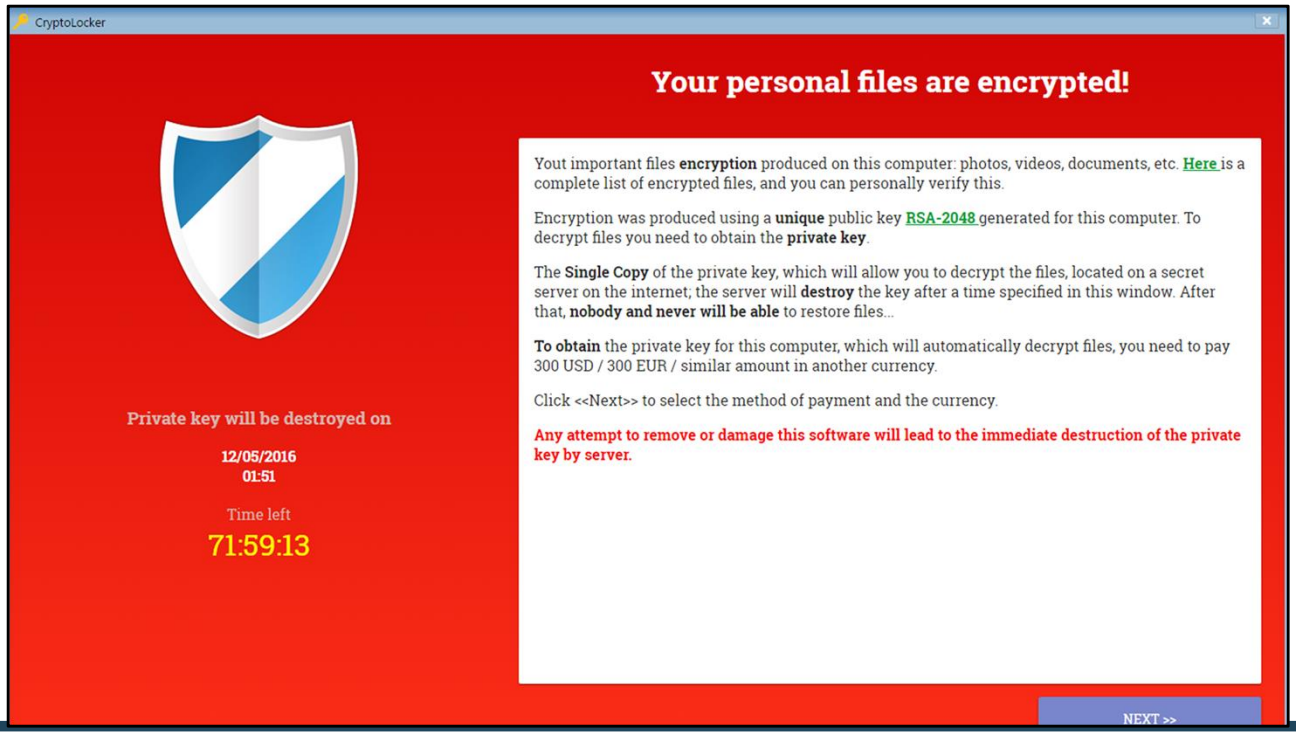
There are numerous ways that attacks and incidents can occur. Some malicious some accidental. No industry is safe.



KEY POINTS

There are numerous devices and systems types that have to be consideredwhen thinking about a casino's IT secuity. Each with it's own unique points of interest.

Remember no devices or Operating Systems is completely secure



KEY POINTS

CryptoLockers are a type of Ransomware.

Remember to perform daily backups of critical systems.

Attacks, Tools and Terminology

Denial of Service (DoS)

- Denial of Service or (DoS) or Distributed Denial of Service Attacks (DDoS)
- Deny service to the intended machine or network resource
- Can originate from multiple sources
- Made famous by "hacktivists"
- Defenses?

**2017 WannaCry DDoS attack affected IIS on legacy XP and 2003 systems

KEY POINTS

Not all types of attacks are to steal money or data. Sometimes disruption is the goal. DoS attacks fall under that category.


Malware Defense Techniques
Defense best practices
Update software
• Patches, Hotfixes
• Firmware updates
Watch what you click.
• Adware / TLDR
• Suspicious links
• Suspicious attachments
Antivirus software
• Utilize a firewall
• Install anti-malware software
Use trusted sources.
• Vetted Vendors
• Not all App stores are created equal
Logical security
• Restrict access
• Segregate networks, VLANs

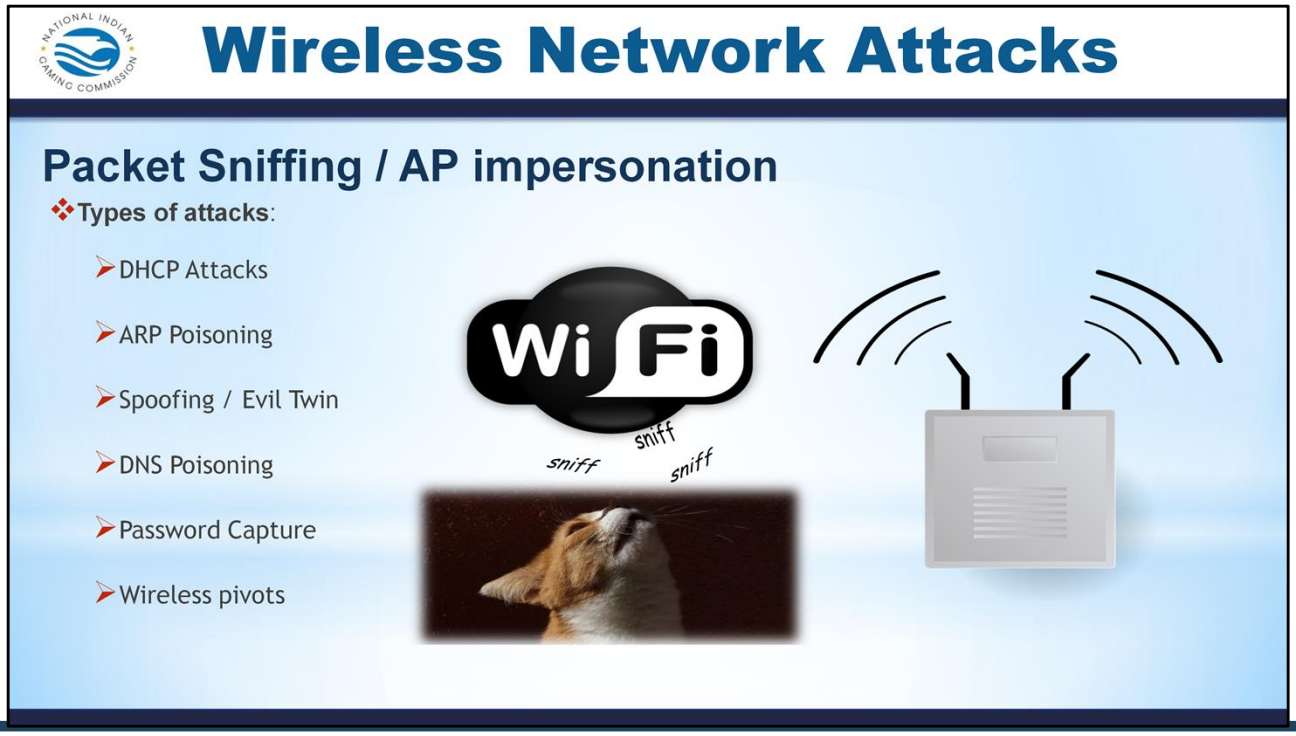
KEY POINTS

KEY POINTS

Activity:

Break into groups. Discuss in groups the types of dangers with each family of systems.

* Remember not all IT vulnerabilities involve a personal computer.



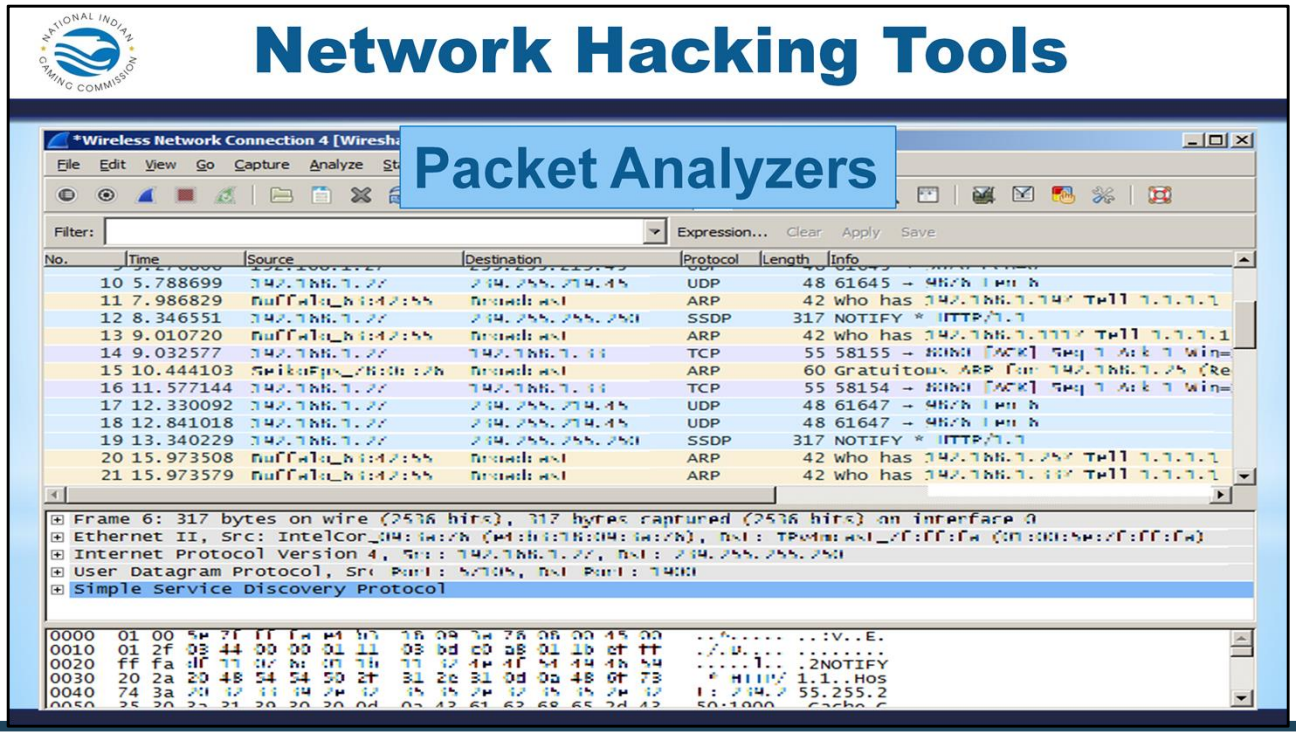
KEY POINTS

A variety of attacks and vulnerabilities exist.

Not all encryption methods are created equally.

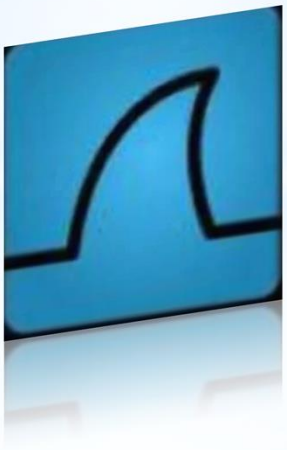
(ie. WPA2-EAP-TLS >> WPA2-EAP-PEAP/EAPTTLS. >> WEP2)

*When possible have a system with separate authenticator and authentication server.

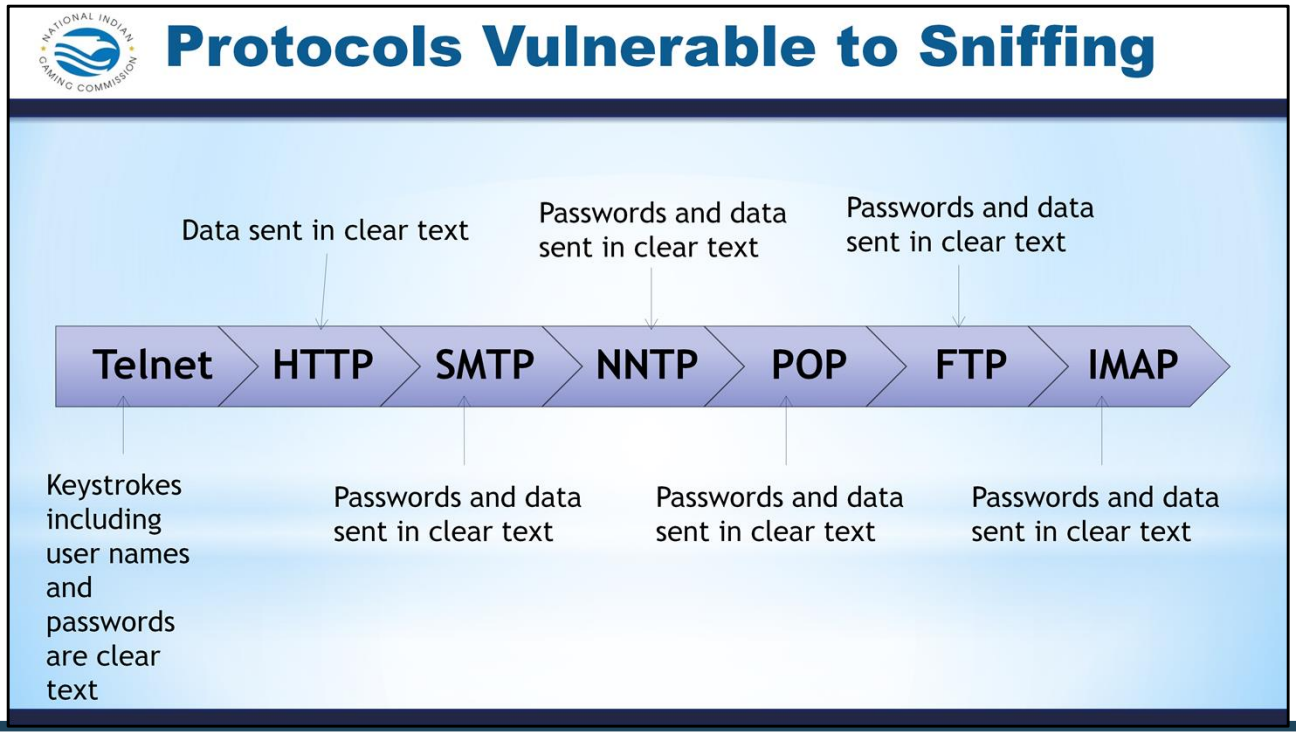

Network Hacking Tools
Packet Analyzers
*Wireless Network Connection 4 [Wiresh
File Edit View Go Capture Analyze
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
10 5.788699 UDP 48 61645 → 9626 Len=6
11 7.986829 ARP 42 who has 192.168.1.192 Tell 1.1.1.1
12 8.346551 SSDP 317 NOTIFY * HTTP/1.1
13 9.010720 ARP 42 who has 192.168.1.1111 Tell 1.1.1.1
14 9.032577 TCP 55 58155 → 8000 [ACK] Seq=1 Ack=1 Win=
15 10.444103 ARP 60 Gratuitous ARP for 192.168.1.25 (Re
16 11.577144 TCP 55 58154 → 8000 [ACK] Seq=1 Ack=1 Win=
17 12.330092 UDP 48 61647 → 9626 Len=6
18 12.841018 UDP 48 61647 → 9626 Len=6
19 13.340229 SSDP 317 NOTIFY * HTTP/1.1
20 15.973508 ARP 42 who has 192.168.1.252 Tell 1.1.1.1
21 15.973579 ARP 42 who has Tell 1.1.1.1
Frame 6: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface 0
Ethernet II, Src: IntelCor_04:1a:26
Internet Protocol Version 4, Src: 192.168.1.22, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57105, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa
0010 01 2f 03 44 00 00 01 11
0020 ff fa
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73
0040 74 3a
..:V..E.
.2NOTIFY
* HTTP/1.1..Hos
t: 239.255.255.2

KEY POINTS

Activity – Wireshark Demo



KEY POINTS



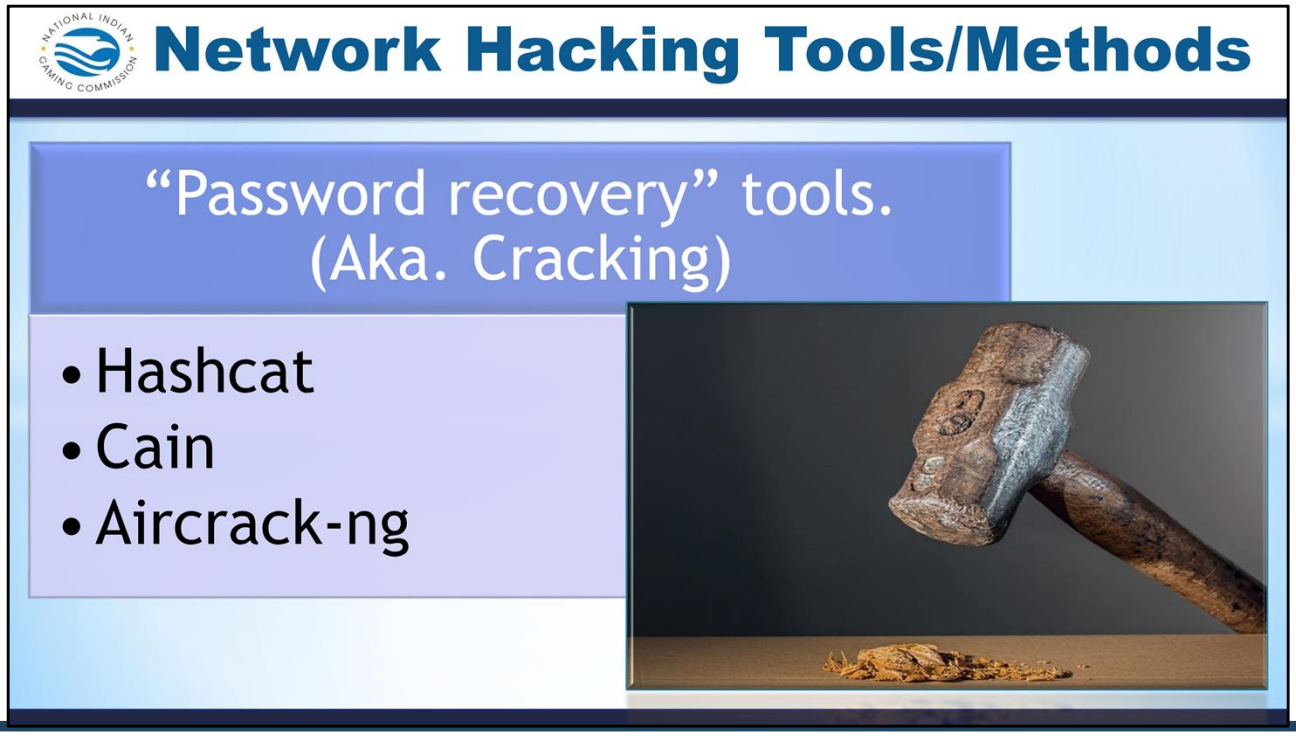
KEY POINTS

Use encrypted transmission methods whenever possible.

Packet Sniffing Defenses

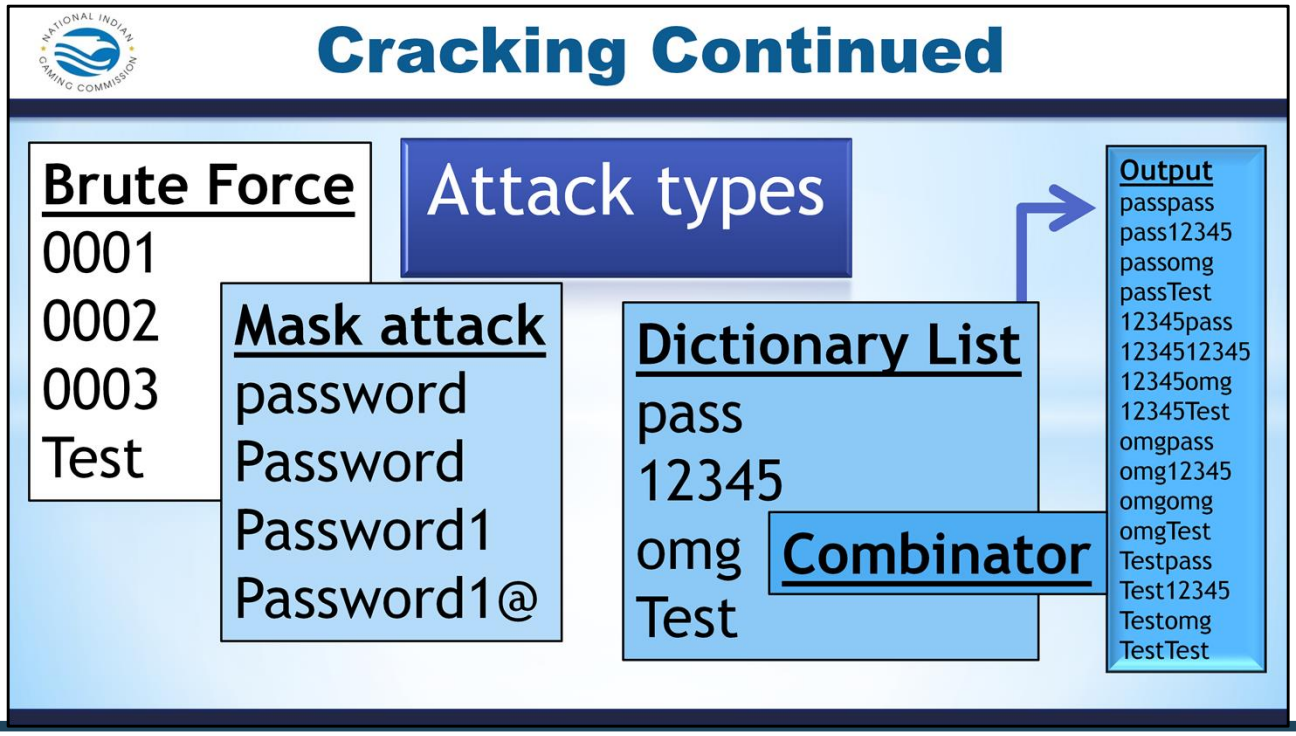
- **Restrict** physical access to the network.
- Use **encryption**.
- **Use MAC addresses.**
- Use **static IP address and static APR**
- **Turn off** network identification broadcasts (ESSIS / BSSID)
- Use **IPv6** instead of IPv4 protocol.
- Avoid **outdated** Access Point encryption methods such as **WEP** encryption!

KEY POINTS



KEY POINTS

A variety of cheap free and easy to use password cracking tools exist



KEY POINTS

Different password guessing strategies exist and can easily be combined

Cracking Continued

Hash Decryption

- MD4, MD5
- SHA1
- SHA-256, SHA-512
- SHA-3 (Keccak)
- OSX v10.10
- AIX {ssha512}
- Cisco-ASA MD5
- Juniper IVE
- Samsung Android Password/PIN
- Windows Phone 8+ PIN/password
- PDF 1.7 Level 8 (Acrobat 10 - 11)
- MS Office 2013
- Bitcoin/Litecoin wallet.dat
- Blockchain, My Wallet, etc.

KEY POINTS

Most encryption methods have ways of being decrypted therefore choose a strong method, a strong password, and change passwords often.

Human Error

Carelessness

Example of June 2017 publishing of data on 200 million US citizens by Deep Root analytics

Data was left exposed on a database in an unsecured, publicly accessible Amazon Web Services S3 bucket

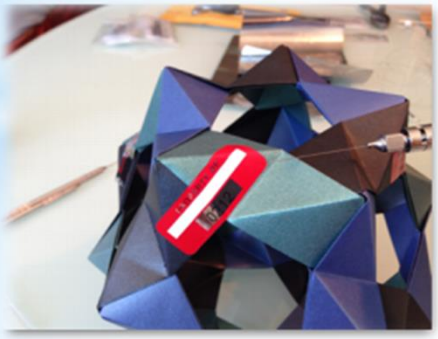
KEY POINTS

Sometimes vulnerabilities and data loss come from external or internal attackers, and sometimes from lack of education.

Human Error – Tamper Proof

Note: A tremendous variety of seals can be removed and reapplied with only:

- Naphtha
- Syringe
- X-Acto knife
- Nitrile gloves



KEY POINTS

Serialized, tamper evident seals are useful but only when paired with random file signature checks.
Simple techniques exist to hack both adhesive based and non-adhesive based seals.

Human Error–Social Engineering

The art of convincing people to reveal confidential information.

Phases in a Social Engineering Attack

- **Research Target Company**
  Dumpster diving, websites, employees, tour company, etc.
- **Select Victim**
  Identify a frustrated employee
- **Develop Relationship**
  Build some type of personal relationship with the selected employee
- **Exploit**
  Collect sensitive personal information (kids' names, birthdays), financial information or current company technologies

KEY POINTS

Human Error–Social Engineering

Phishing

- Designed to fraudulently obtain private information
- Generally, does not involve personal contact, usually legitimate looking E-mail, websites, or other electronic means are involved in phishing attacks. (ie. QR codes. USB thumb drives, etc)

From: Ioa@Citizensbank.com [mailto:Ioa@Citizensbank.com]
Sent: Wednesday, August 25, 2004 11:57 PM
To: [redacted]
Subject: Citizensbank.com acount holdtq

CITIZENS BANK
Not your typical bank.®

Security key: qjkjaxaqwrq

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
https://www.citizensbankonline.com/banking/verification-process1.html
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citizens Bank Business Development; this process cannot be externally requested through Customer Support.

Sincerely,
Citizensbank.com
Business Department.

KEY POINTS
Phishing can be email based but also via phone.

Human Error–Social Engineering

Persuasion

Hackers employ social engineering from a psychological point-of-view

Basic methods include:

- impersonation
- conformity
- diffusion of responsibility (Not my job)
- plain old friendliness

KEY POINTS

Conformity – people naturally avoid confrontation
Diffusion of responsibility – It's not my problem. Not my job.
Friendliness – Name dropping, gathering info (your favorite team, your first car)

Human Error–Social Engineering

On-Line Social Engineering

- The Internet is fertile ground for social engineers looking to harvest passwords
- Many users often repeat the use of one simple password on every account: Yahoo, Travelocity, Gap.com, etc.
- Once the hacker has one password, he or she can probably get into multiple accounts
- Large amounts of personal data are on the social sites as well

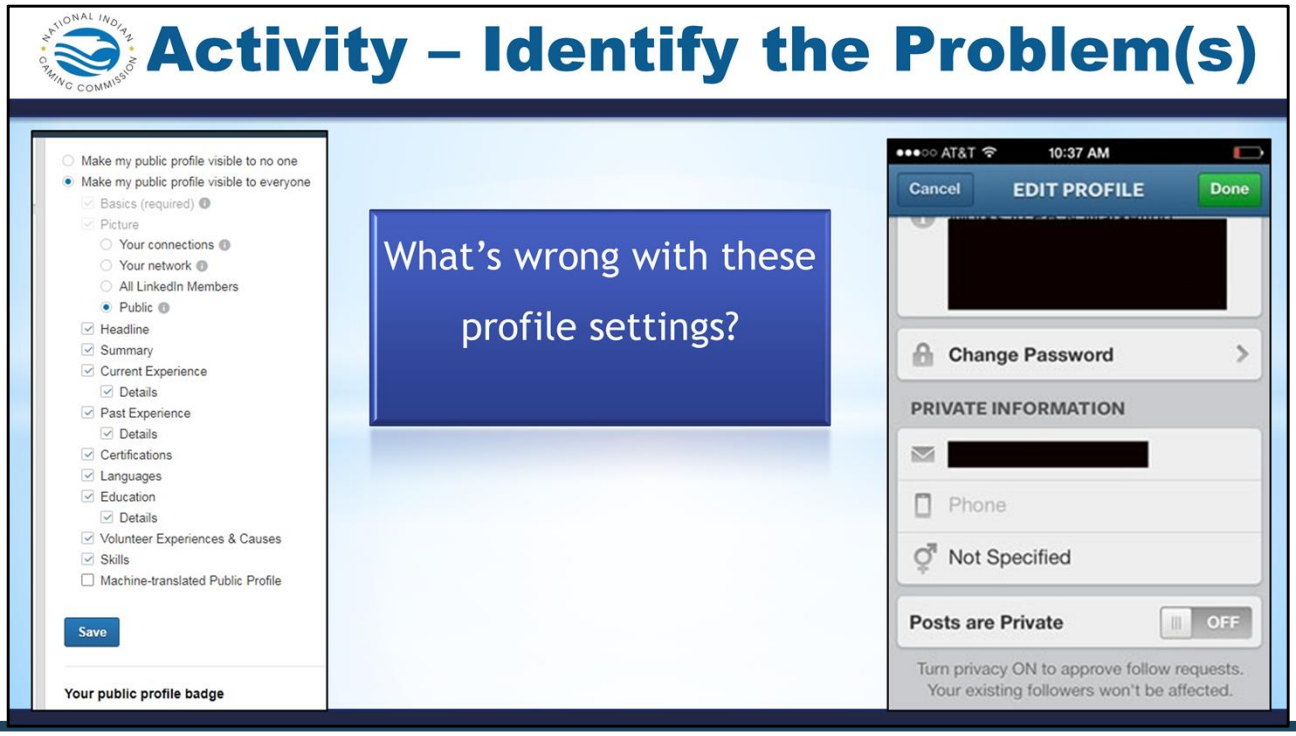
KEY POINTS

Human Error – Social Media

Tips for securing your online profile

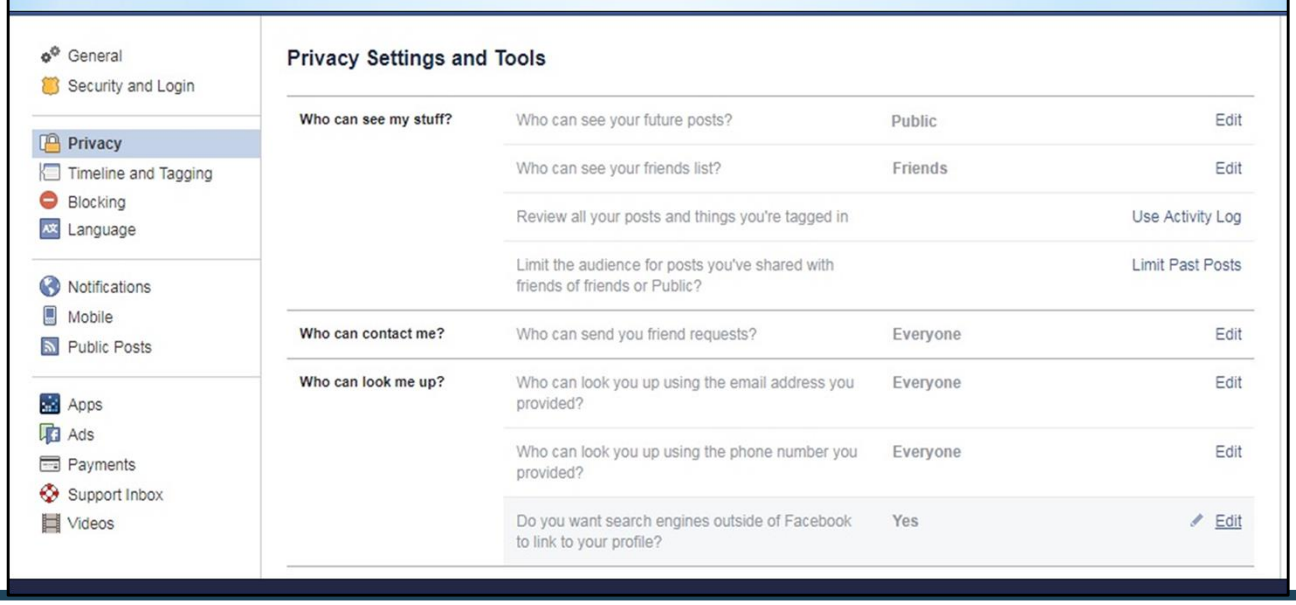
> Carefully choose your audience. (Friends, friends of friends, public)
> Use a Secret Email Address
> Secure Those Security Questions
> Set Up Login Notifications (dual factor auth)
> Don't link accounts

KEY POINTS

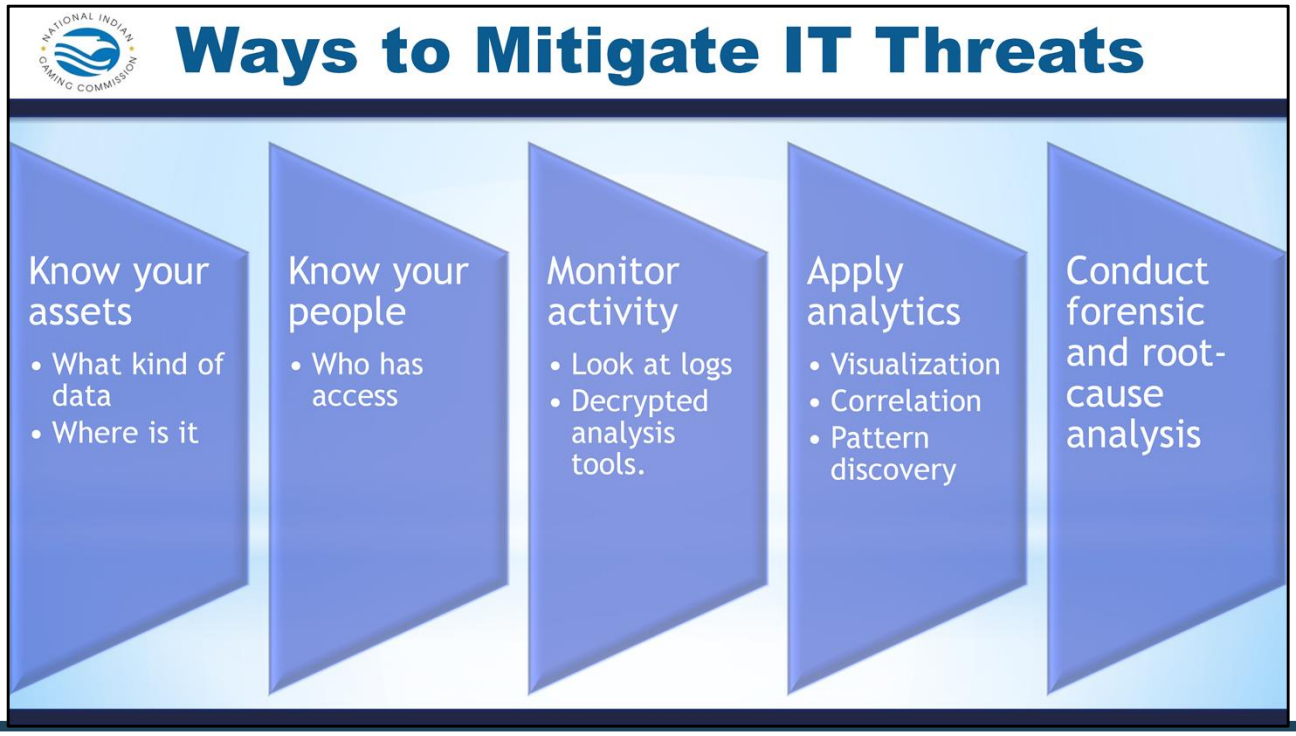

Activity – Identify the Problem(s)
Make my public profile visible to no one
Make my public profile visible to everyone
Basics (required)
Picture
Your connections
Your network
All LinkedIn Members
Public
Headline
Summary
Current Experience
Details
Past Experience
Details
Certifications
Languages
Education
Details
Volunteer Experiences & Causes
Skills
Machine-translated Public Profile
Save
Your public profile badge
What's wrong with these profile settings?
AT&T
10:37 AM
Cancel
EDIT PROFILE
Done
Change Password
PRIVATE INFORMATION
Phone
Not Specified
Posts are Private
OFF
Turn privacy ON to approve follow requests.
Your existing followers won't be affected.

KEY POINTS

Activity – Identify the Problem(s)



KEY POINTS


Ways to Mitigate IT Threats
Know your assets
• What kind of data
• Where is it
Know your people
• Who has access
Monitor activity
• Look at logs
• Decrypted analysis tools.
Apply analytics
• Visualization
• Correlation
• Pattern discovery
Conduct forensic and root-cause analysis

KEY POINTS

On the Horizon

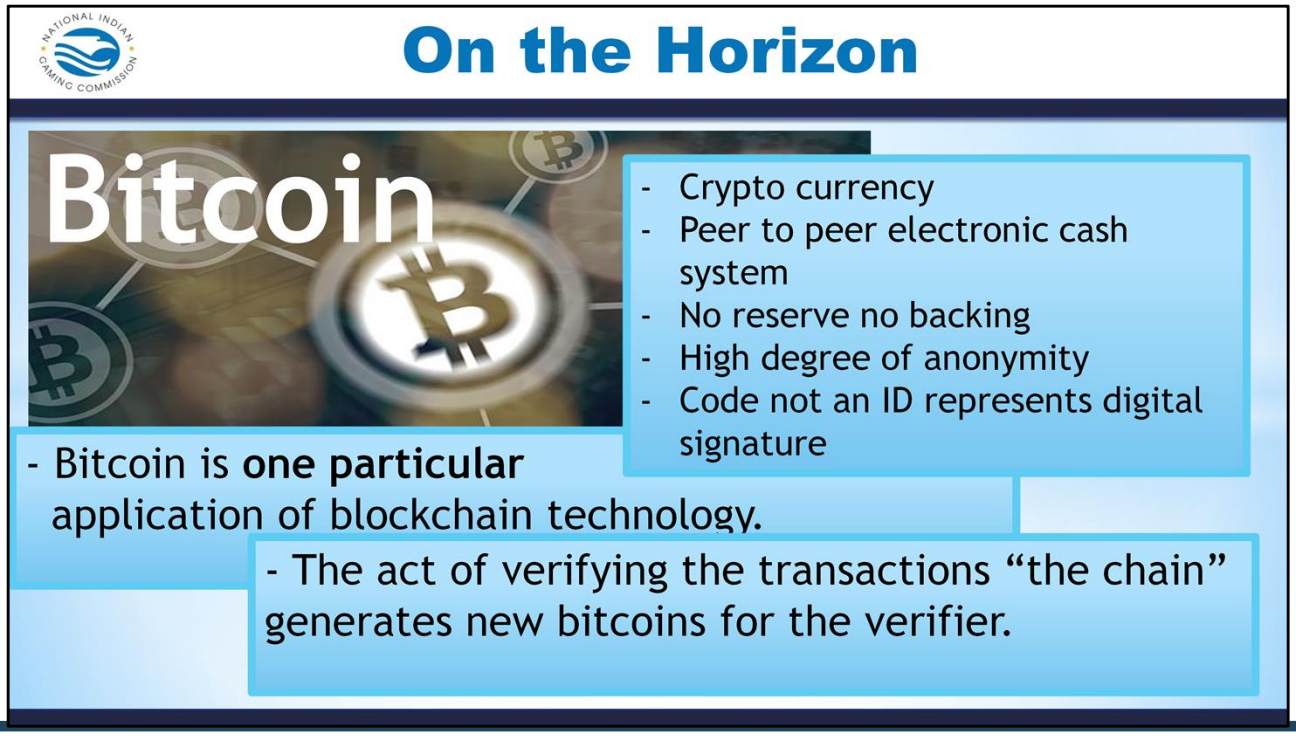
Blockchains, Bitcoin, Ether, and Crypto-currencies

What are blockchains?

-> Blockchain is to Bitcoin, what the internet is to email
-> A large electronic system on which you can build applications.
-> A distributed database that is used to maintain a continuously growing list of records, called blocks.
-> A peer-to-peer network collectively adhering to a protocol for validating new blocks.
-> Data is stored across, processed, and validated by the devices across the network.

KEY POINTS

Blockchain technology is new and rapidly developing.
Blockchain is to Bitcoin, what the internet is to email.



KEY POINTS

- Relevant to casinos as the potential exists for money laundering.
- Illegal marketplaces.

On the Horizon

Etherium and Smart Contracts

> Etherium is a usage of blockchain technology. Mining ether cryptocurrency
> Etherium focuses on running the programming code of a decentralized application not just currency.
> Smart Contracts are self operating computer programs that operate on the blockchain.

Uses and **Dangers** of (Dapp) Decentralized applications:

> Not controlled by individual
> Immutable, zero downtime, tamperproof
> Difficult to correct.
> Private blockchains potentially susceptible to group corruption

KEY POINTS

Crypto coin technology will likely become more prevalent in other industries and scenarios.

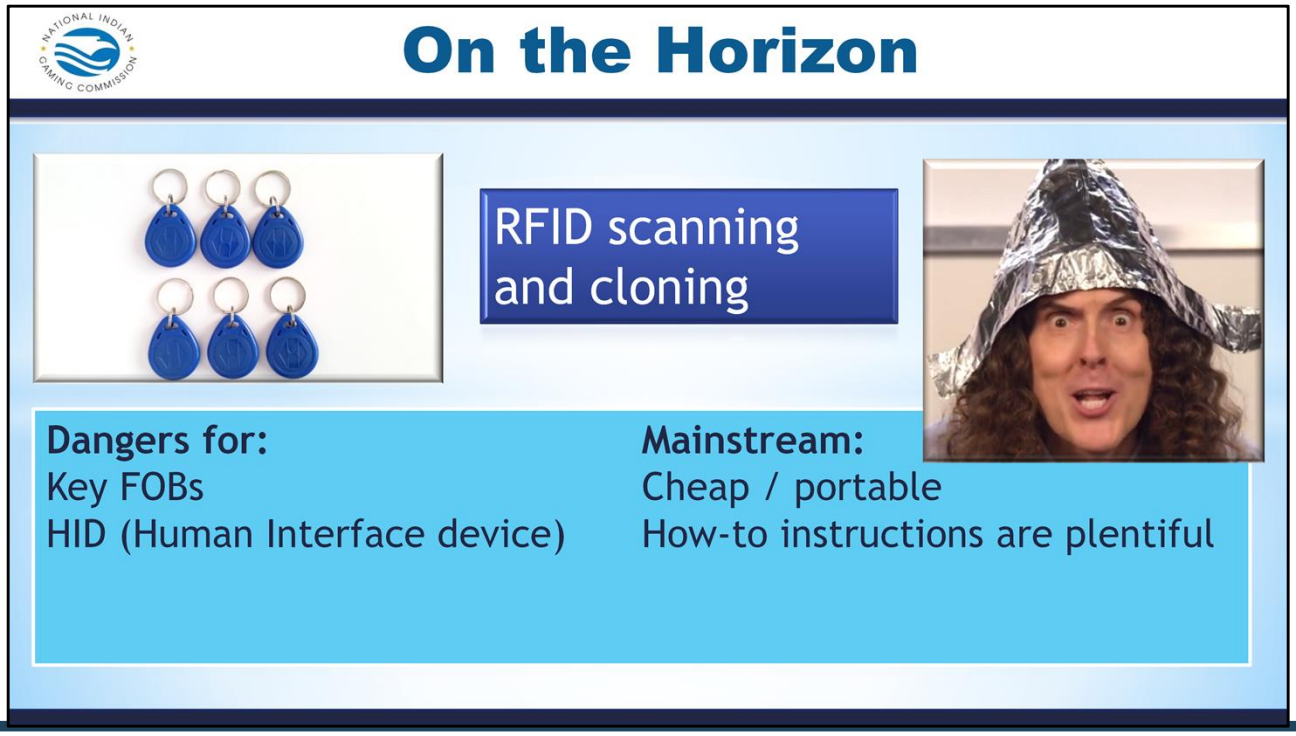
On the Horizon

Facial recognition

- Rapidly evolving technology
- Benefits of combating theft, trafficking
- Used for biometric identification and eventually payments
- Potentially combined with other tech such as drones

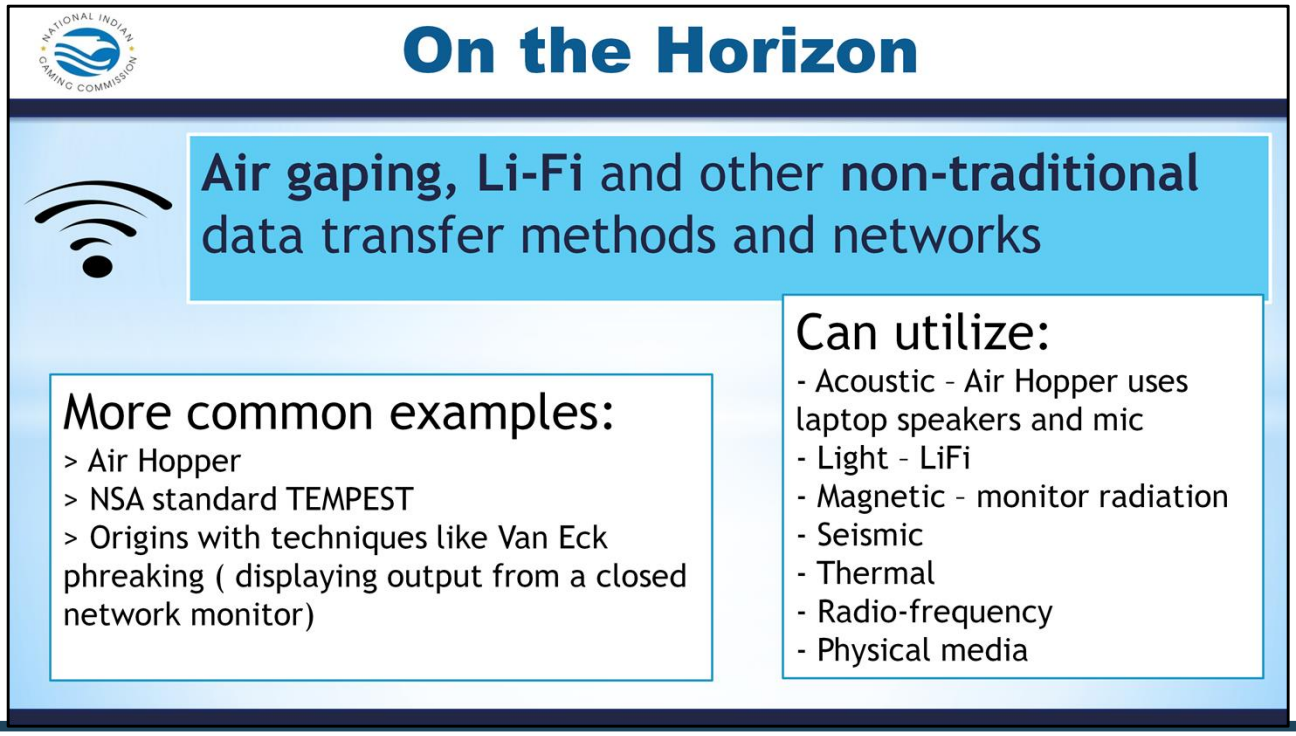
Source: http://www.bbc.com

KEY POINTS



KEY POINTS

Don’t rely on key management systems alone. Other controls are required.

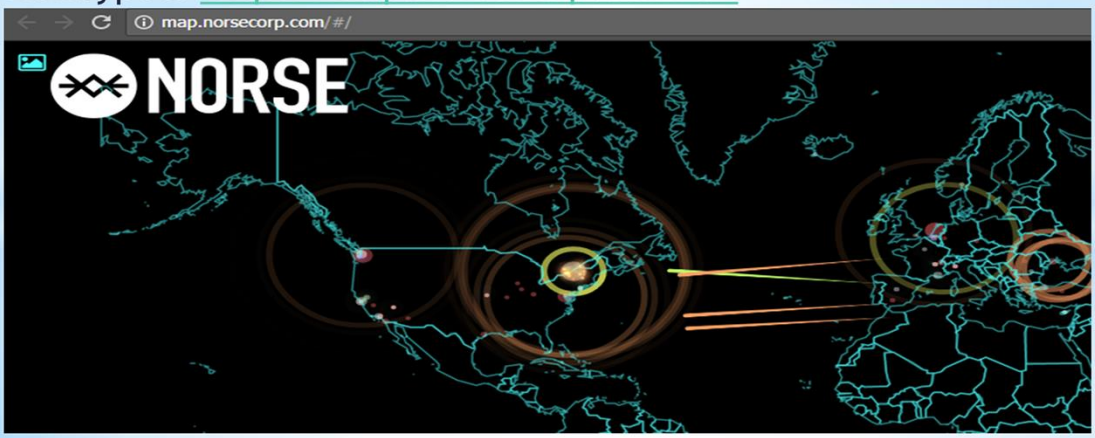


KEY POINTS

Technologies evolve, and not all data is sent via WiFi or other networks.

On the Horizon

Honeypots http://map.norsecorp.com/#/



KEY POINTS

Questions

Tim Cotton
IT Auditor
timothy_cotton@nigc.gov

Jeran Cox
IT Auditor
jeran_cox@nigc.gov

Michael Curry
IT Auditor
michael_curry@nigc.gov

Sean Mason
IT Auditor
sean_mason@nigc.gov

Travis Waldo
Director, IT
travis_waldo@nigc.gov

KEY POINTS


Course Evaluation
• Provide an honest assessment of your experience
• Written suggestions and comments are greatly appreciated and allow us to improve your experience

KEY POINTS

KEY POINTS

Poll Title: Course Eval IT-108 IT Threats

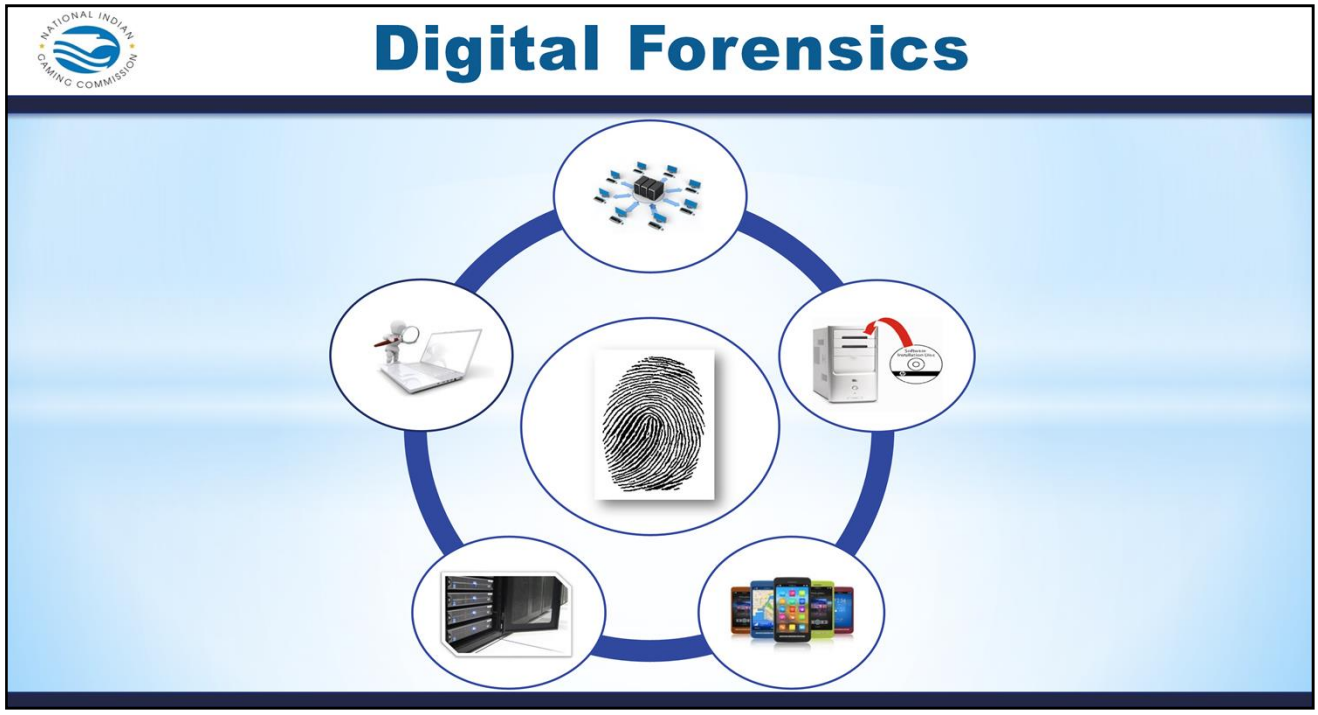
https://www.polleverywhere.com/surveys/Em2QWMJXh

IT-107 Gaming Forensics

IT-107 Gaming Forensics

Information Technology Division

KEY POINTS



KEY POINTS

1. Network Forensics
2. Computers
3. Mobile Devices
4. Database
5. Live


Course Overview
WHAT?
• Common Types
• Investigations
WHY?
• Chain of Custody
• Evidence Gathering
WHO?
• First Responders
• Gaming Commissions
HOW?
• Plan of Action
• Collected Evidence

KEY POINTS

KEY POINTS

Poll Title: Has anyone gone through a forensic with an ITL?

https://www.polleverywhere.com/multiple_choice_polls/TV3tvEM9ndVGHB9

KEY POINTS

1. Criminalistics are the study and collection of physical evidence at the crime.
2. Video Analysis is the scientific study and collection of video for legal matters.
3. Accounting is the study and analysis of collection of financial evidence.

KEY POINTS

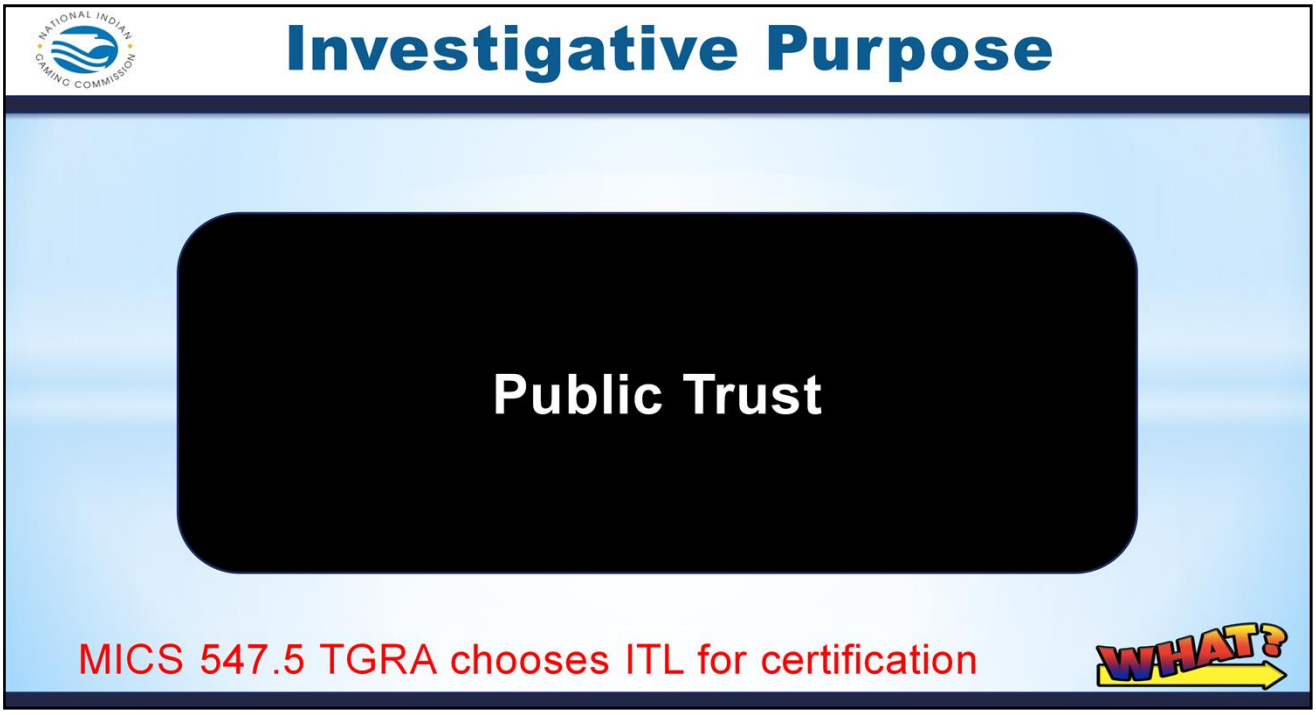
In the regulated gaming arena, a forensic investigation typically occurs when gaming or associated equipment has malfunctioned or performed an operation outside the range of that equipment's programmed abilities

Common Types

- Non-existent payline or bonus awards
- Physical reel strip vs. prize/award mismatch
- Credit award not present within prize schedule
- Electromechanical fault (reels continue to spin)
- External bonus awarded to selected player accounts
- Physical tampering (electrical shock or interference)
- Backend system manipulation – new investigating further

WHAT?

KEY POINTS



KEY POINTS

Why are forensic investigations and relevant procedures important?

- For instituting a set of operational forensic procedures regarding security of evidence
- For establishing communication and proper procedures between the regulatory bodies, operators, and independent testing laboratories
- To help in maintaining service and continuity between gaming departments by isolating the incident
- For recognizing, investigating and responding to incidents. This will also help with mitigating future risks!
- Maintaining public trust (damage control!)

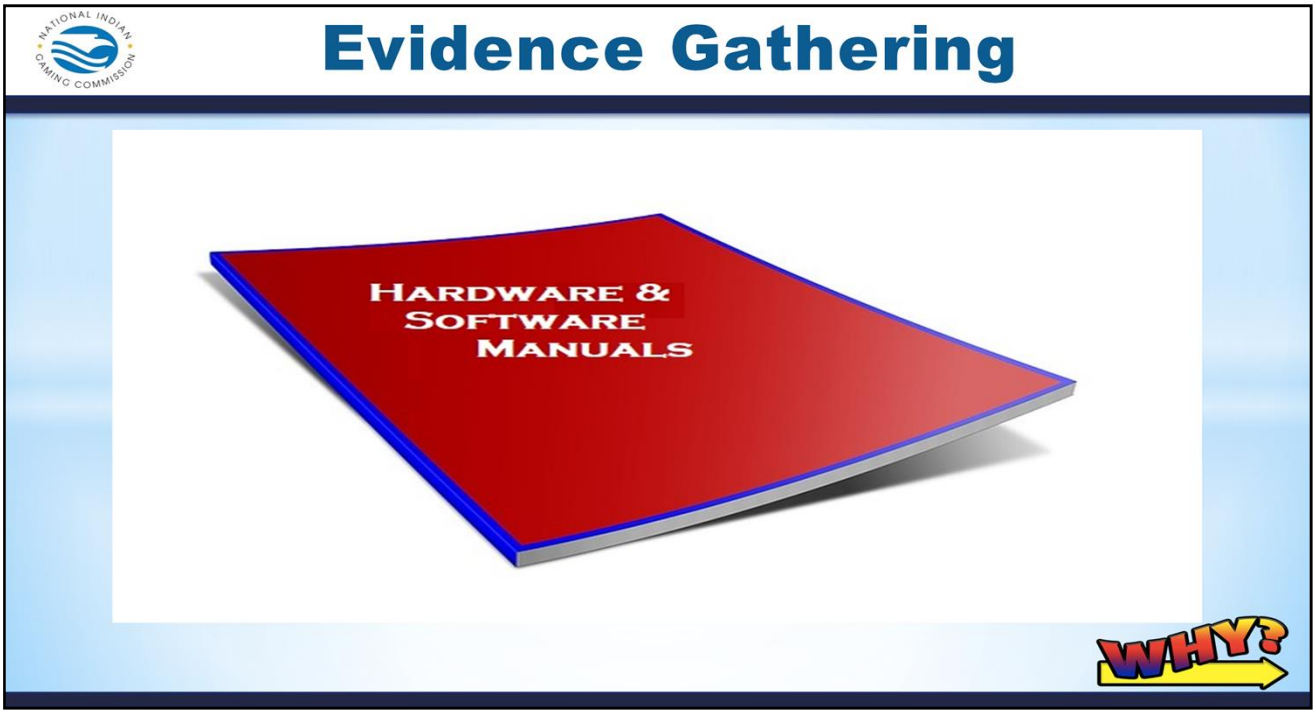
Chain of Custody

Include:

- Inception - Evidence Collection
- Paper Trail
- Integrity of evidence until processed
- TGRA &/or Regulatory body determine extent of actions
- Best Practice Guideline
  - US DOJ (Justice) / NIST(National Institute of Standards and Technology

KEY POINTS

Chain of Custody is vital in the event that a dispute goes to court.



KEY POINTS

Examples of physical/non-electronic evidence include:

- Ticket cash receipts and jackpot/regular vouchers
- Photographs of gaming and associated equipment
- Gaming Machine/Terminal cabinet
- Machine Entry Authorization Log Book (MEAL Book) and Progressive Entry Authorization Logs (PEAL)
- Key Control logs

Examples of physical/non-electronic evidence include:

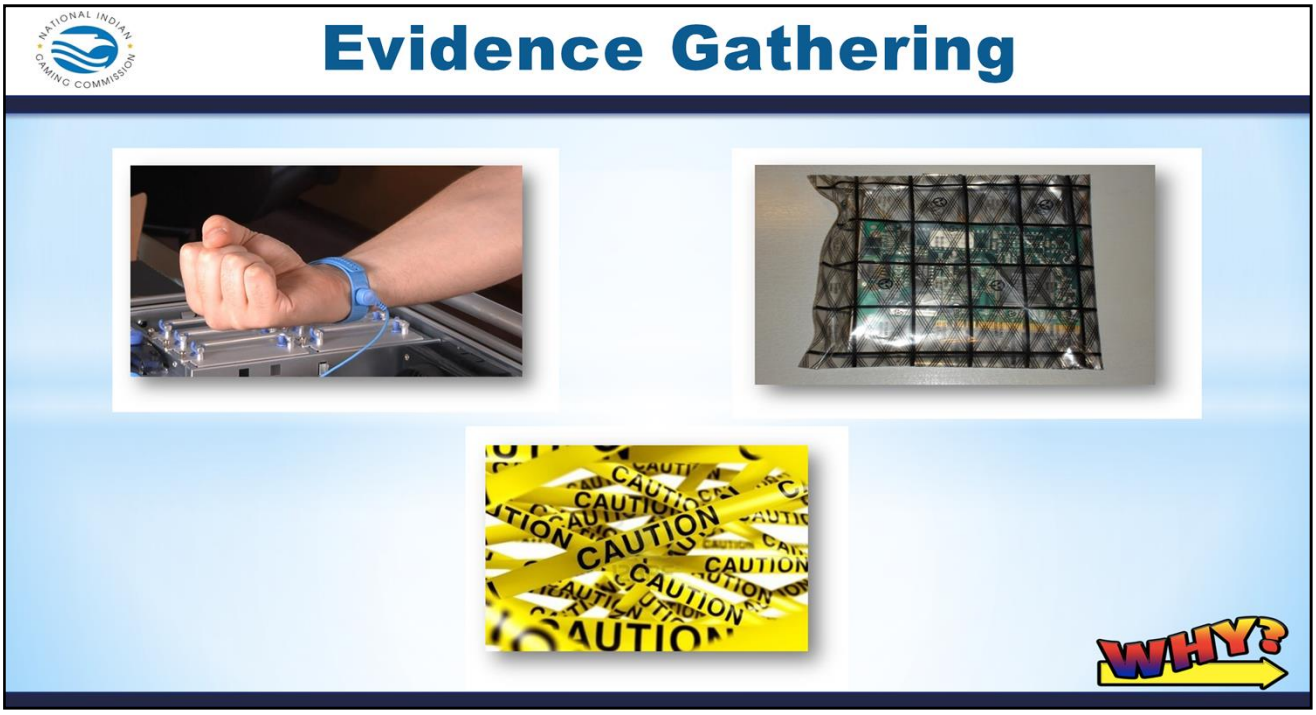
- Miscellaneous handwritten notes (for example, comments written down during previous service)
- Player Promotional Cards
- Tools possibly used to compromise the gaming equipment (screwdrivers, rods, magnets, taser, etc.)
- Hardware and software manuals
- Server/System Generated Reports (Door Entry, Metering, etc.)

KEY POINTS

Examples of electronic evidence include:

- Hard drive/Hard drive data
- CDs, DVDs, or other optical storage devices
- USB Flash Drives, Compact Flash cards, or other flash memory storage devices
- Wireless Devices
- EPROMs with or without logic boards

Incidents may not involve gaming equipment, but other parts of the gaming floor. Evidence associated with these incidents include:



KEY POINTS

Have a “crash cart”
Protect yourself and equipment from static discharge.

First Responders

Those directly affecting gaming integrity

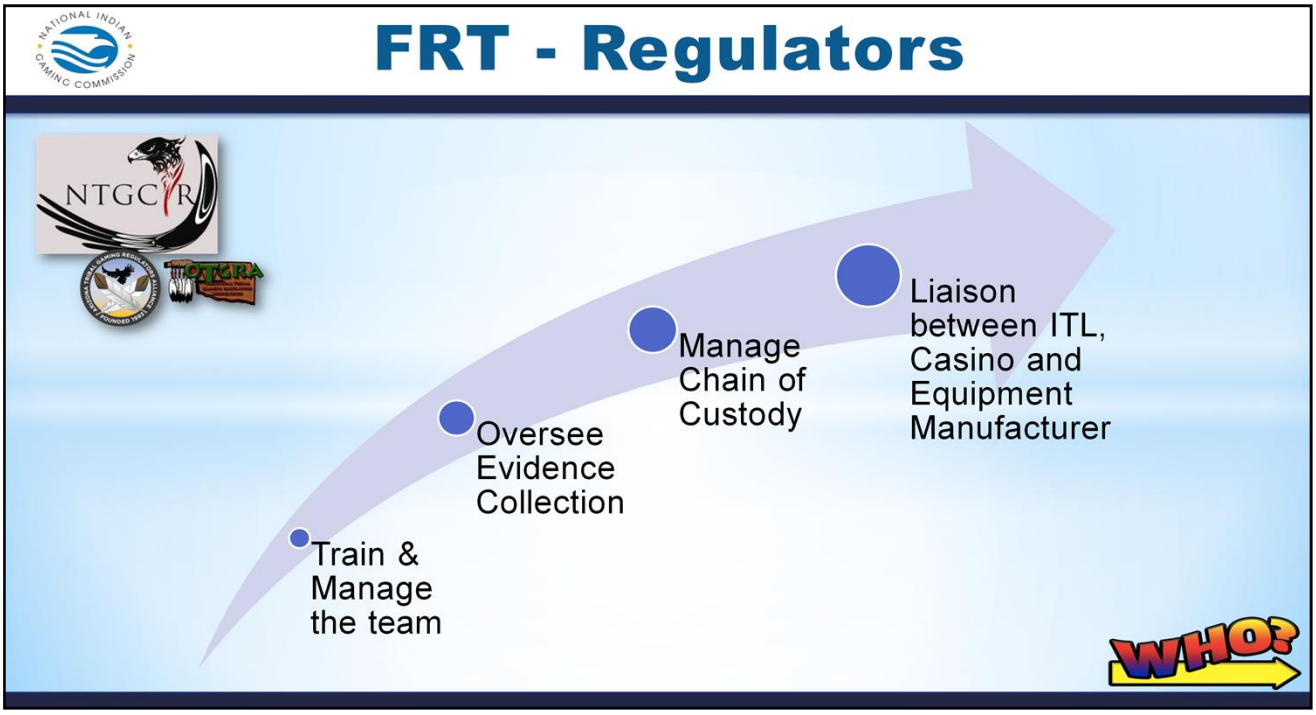
- ❑Regulators
- ❑Gaming Operations
- ❑Information Technology
- ❑Security
- ❑Surveillance
- ❑Accounting and Auditing

KEY POINTS

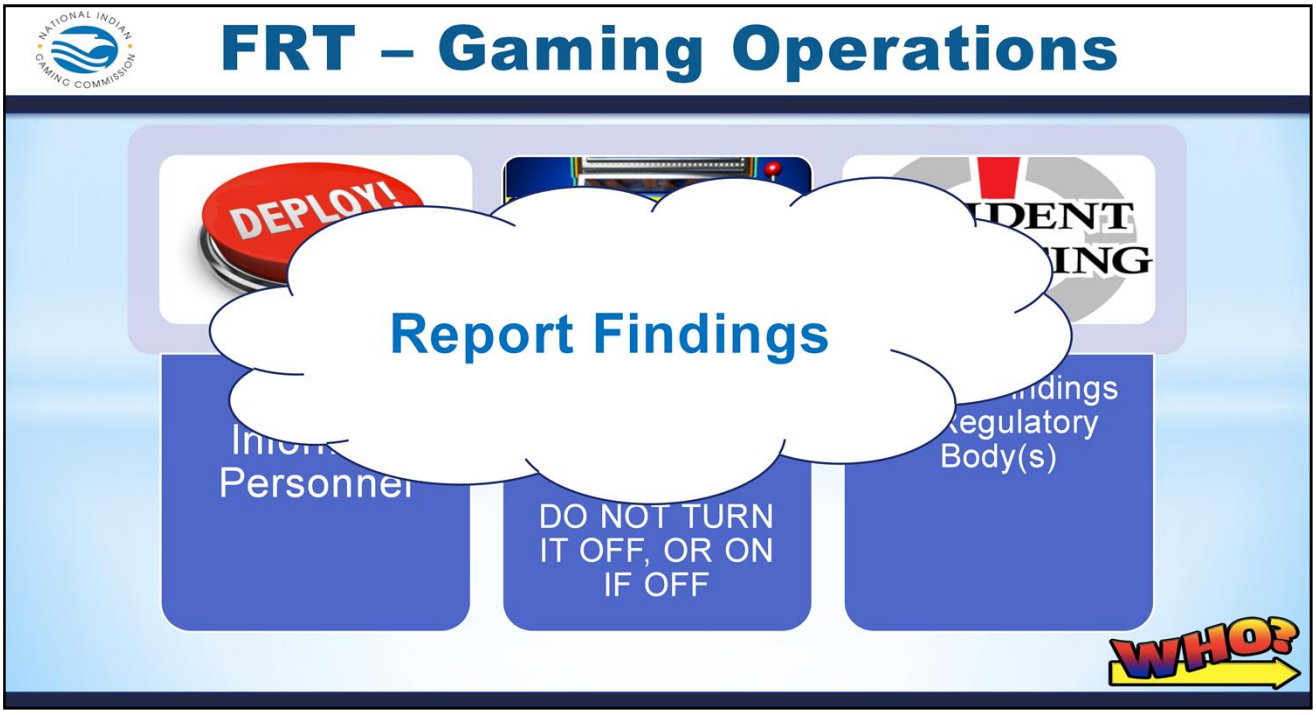
KEY POINTS

Poll Title: Does anyone have a first Responders Team?

https://www.polleverywhere.com/multiple_choice_polls/ifosYLx4hEXGFBB

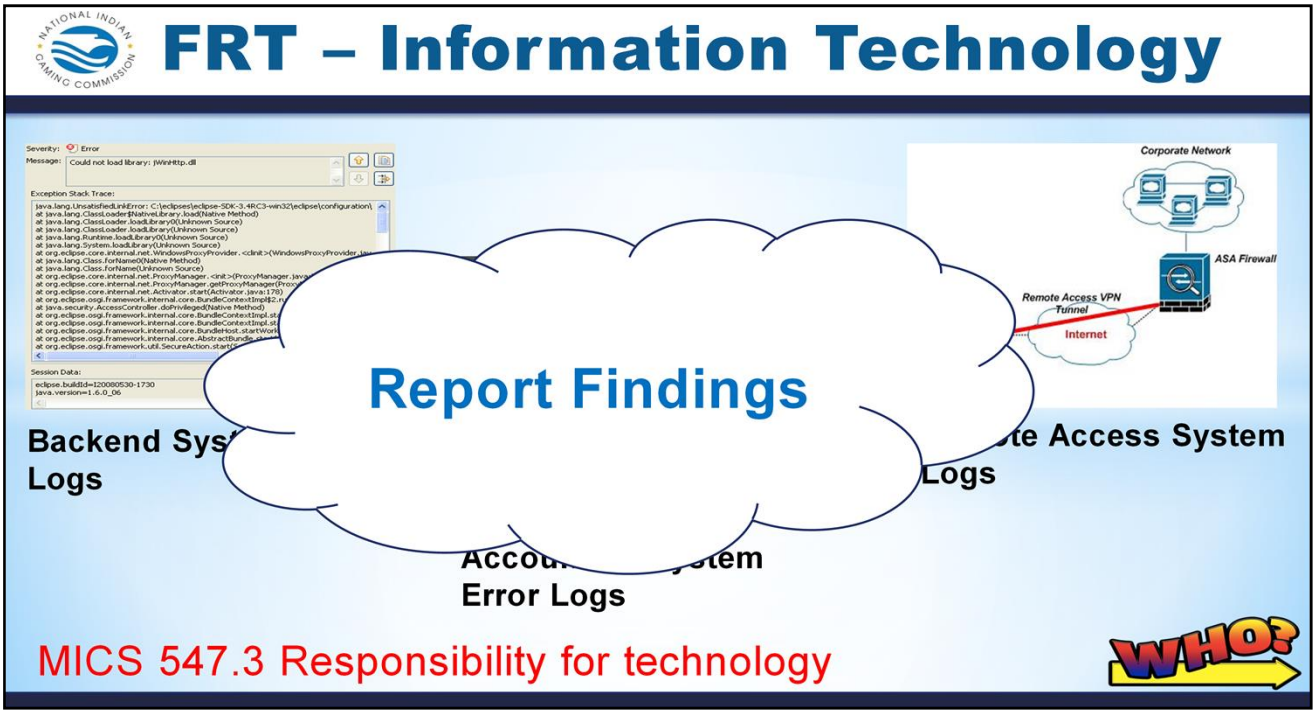

FRT - Regulators
NTGCR
Train & Manage the team
Oversee Evidence Collection
Manage Chain of Custody
Liaison between ITL, Casino and Equipment Manufacturer
WHO?

KEY POINTS



KEY POINTS

DO NOT TURN IT OFF IF ON, OR ON IF OFF

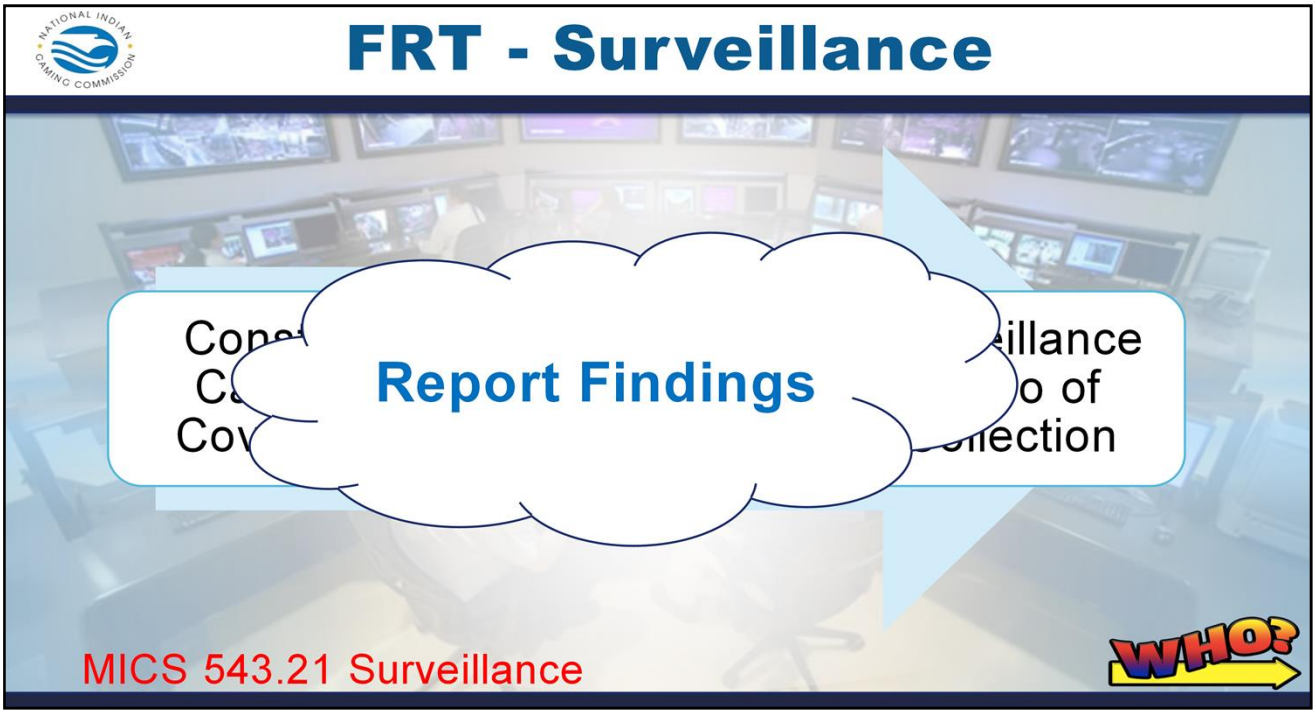


KEY POINTS

The Information Technology Department are the floor gaming equipment communications experts and are responsible for securing all data pertaining to the scene.

KEY POINTS

The Security Department are the people oriented investigation and enforcement expert on the scene and are responsible for:



KEY POINTS

The Surveillance Department are the ever present “eye in the sky” and are responsible for maintaining constant coverage.

KEY POINTS

The Auditing and Accounting Department are the money experts and are responsible for examining tickets.

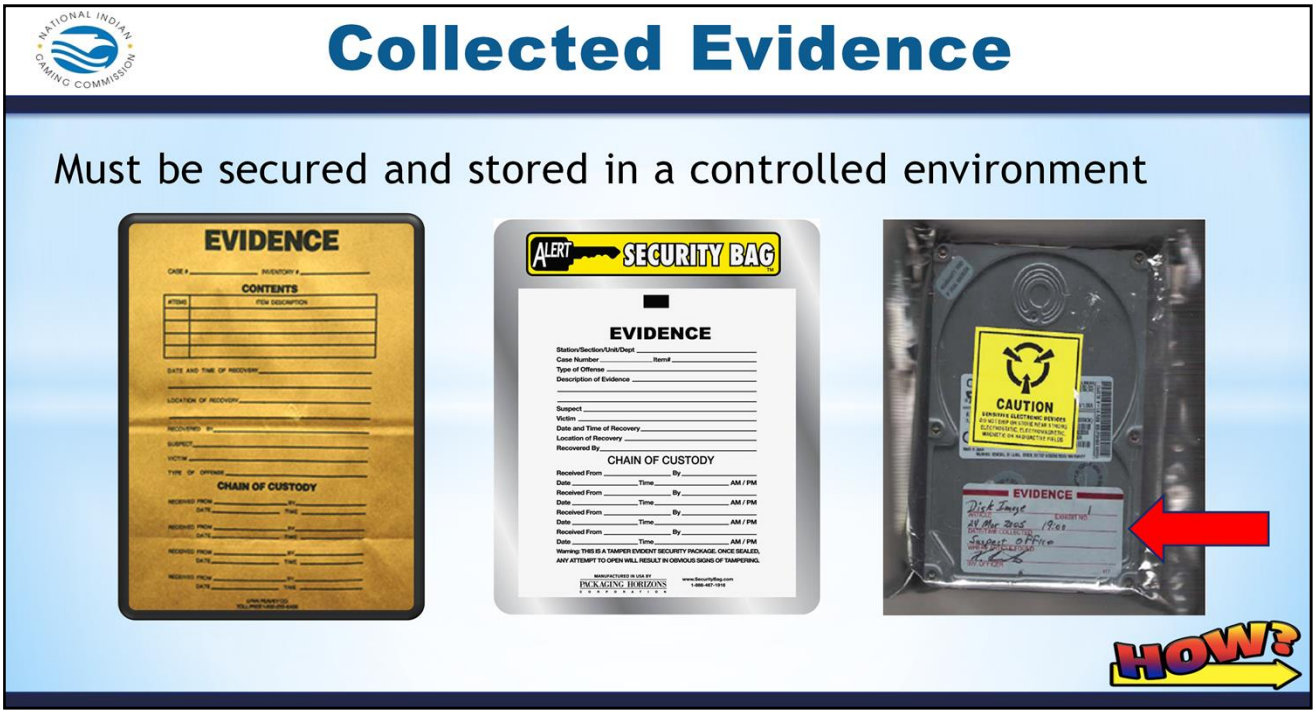

Gaming Commission
As the regulatory body submits information and components for a forensic examination following a thorough investigation and gathering of information and evidence.
SEAL OF THE CHEROKEE NATION
SEPT. 6, 1839
IOWA TRIBE
KANSAS - NEBRASKA
ONEIDA
Gaming Commission
POARCH CREEK INDIANS
WHO?

KEY POINTS

KEY POINTS

What should a forensic plan of action consist of?

- Establishing a First Responder Team?
- Establishing a Forensic Threshold?
- Escalation guidelines?
- Forensic Readiness Training?



KEY POINTS

The transfer from evidence collection to a lab should follow procedures such as:

- Proper packaging
- Shipping
- Evidence Repository
- Line of Communication
- Red Arrow reiterate how much date/time signature of individual(s) and proper chain of custody

Collected Evidence

Areas of concern for gaming operators are:

- Game malfunction for server connected/controlled games (SBG, Server Supported, etc.)
- Verification of Jackpots (Server level vs. terminal level)
- Patron disputes over game outcomes
- "Superuser" type accounts on the player tracking side
- Gaming Equipment or Host Server tampering
- Disgruntled Manufacturers and internal/external (vendor's) IT employees

HOW?

KEY POINTS

Risk Mitigation

Risks factors YOU can control:

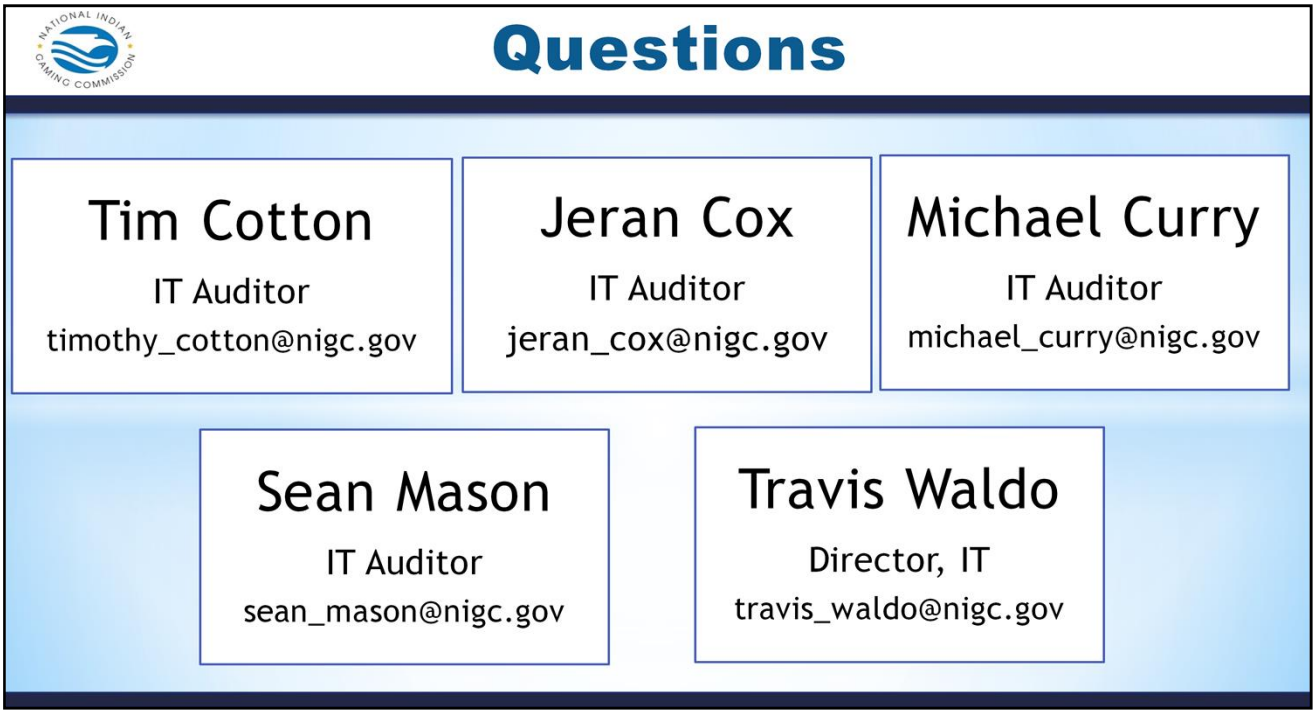
- **Licensure**: Vetting vendors who have remote access
- **Internal user accounts**: does one person have too many access rights (who watches the watchers?)
- **Tape Seal management**: Are all appropriate areas sealed up? Are all seals tracked/accounted for?
- **Proper accounting/reconciliation**: are there any detectable patterns or abnormal behaviors (runaway meters, mismatch to indicate theft, etc.)?

KEY POINTS

WIIFM?

- Understand how to identify when a forensic occurs
- Familiarize yourself with the common types to assist with addressing
- Have a Plan of Action for Forensic events/investigations
- Know your First Responder Team and contact information
- Always review protocols and understand your Risks

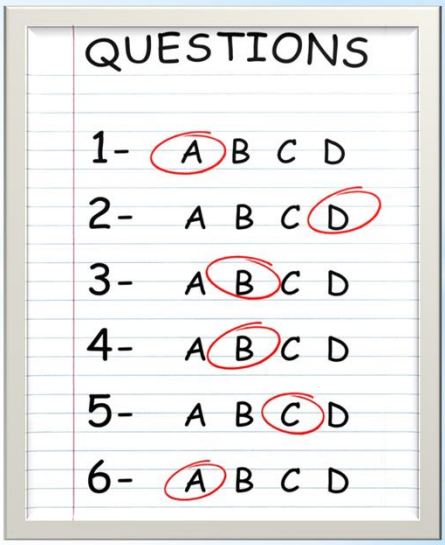
KEY POINTS


Questions
Tim Cotton
IT Auditor
timothy_cotton@nigc.gov
Jeran Cox
IT Auditor
jeran_cox@nigc.gov
Michael Curry
IT Auditor
michael_curry@nigc.gov
Sean Mason
IT Auditor
sean_mason@nigc.gov
Travis Waldo
Director, IT
travis_waldo@nigc.gov

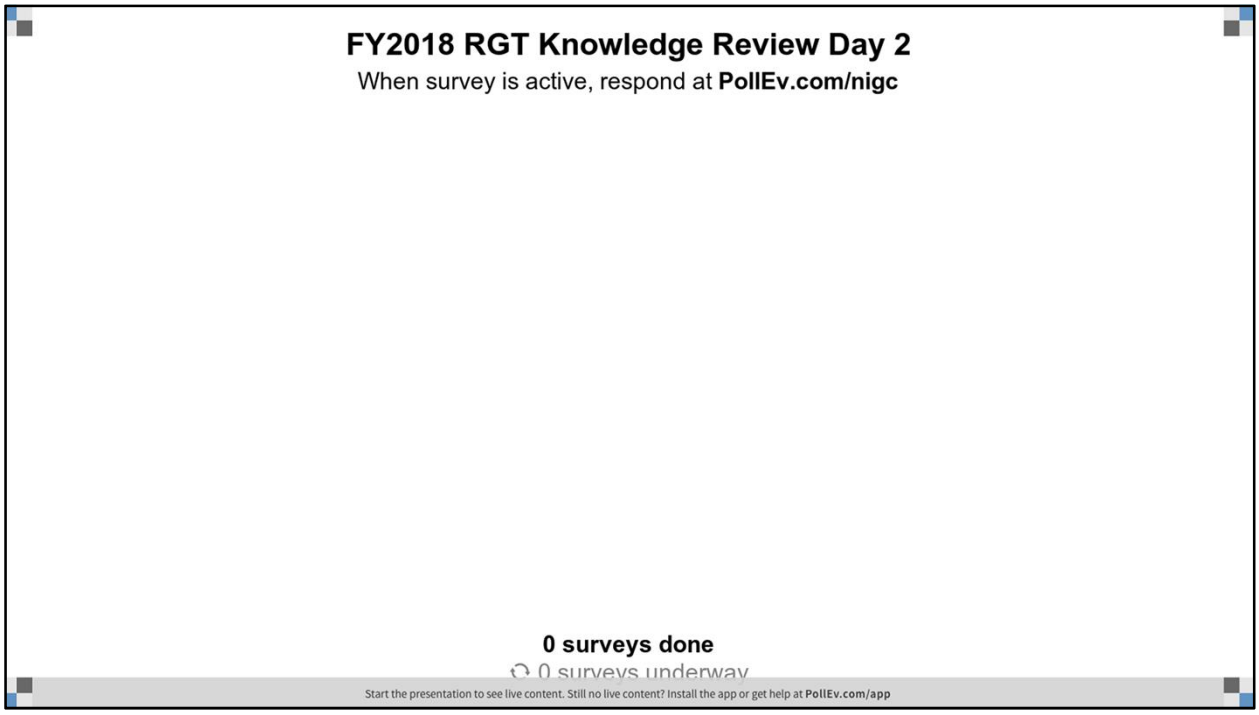
KEY POINTS

Knowledge Review

- Be sure to include your name and email address
- Do your best
- Be on the lookout for the survey email 90 days from today



KEY POINTS



Poll Title: FY2018 RGT Knowledge Review Day 2

https://www.polleverywhere.com/surveys/1Lr00Qis1

Course Evaluation

- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciate and allow us to improve your experience

KEY POINTS

KEY POINTS

Poll Title: Course awe34r567u8i9o0p-[\

IT-107 Forensics in Gaming

https://www.polleverywhere.com/surveys/ZmhFBzBoc