



**Participant Workbook  
Oklahoma City RGT  
Conference  
January 30-31, 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



		<b>OKLAHOMA CITY REGIONAL GAMING TECHNOLOGY</b> <b>January 30th – 31th , 2017</b> Apache Casino Hotel 2315 E Gore Blvd Lawton, OK 73501
<b>Day One</b>	<b>START TIME</b>	
	<b>08:30</b>	Course Opening/Welcome
	<b>09:00</b>	IT-113 IT Basics
	<b>11:00</b>	Break
	<b>11:15</b>	IT-110 Refining and Enhancing your IT TICS
	<b>12:00</b>	<i>Lunch (On your own)</i>
	<b>1:00</b>	IT-110 Refining and Enhancing your IT TICS
	<b>2:00</b>	Break
	<b>2:15</b>	IT-109 Auditing 543
	<b>3:15</b>	Break
	<b>3:30</b>	IT-109 Auditing 543
<b>4:30</b>	<b>Q&amp;A</b>	
		<b>DAY TWO</b>
<b>Day Two</b>	<b>8:30</b>	IT-112 System Verifications & Authentication
	<b>9:30</b>	Break
	<b>9:45</b>	IT-112 System Verifications & Authentication
	<b>10:45</b>	Break
	<b>11:00</b>	IT-108 IT Threats
	<b>12:00</b>	<i>Lunch (On your own)</i>
	<b>1:00</b>	IT-108 IT Threats
	<b>2:00</b>	Break
	<b>2:15</b>	IT-108 IT Threats
	<b>3:15</b>	Break
	<b>3:30</b>	IT-107 Gaming Forensics
<b>4:30</b>	<b>Course Close</b>	

# IT 113 - IT BASICS





# Participant Guide: IT-113 IT Basics

## IT-113 Information Technology Basics



## Information Technology Division

**KEY POINTS**

**My Notes**

# Participant Guide: IT-113 IT Basics

## 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

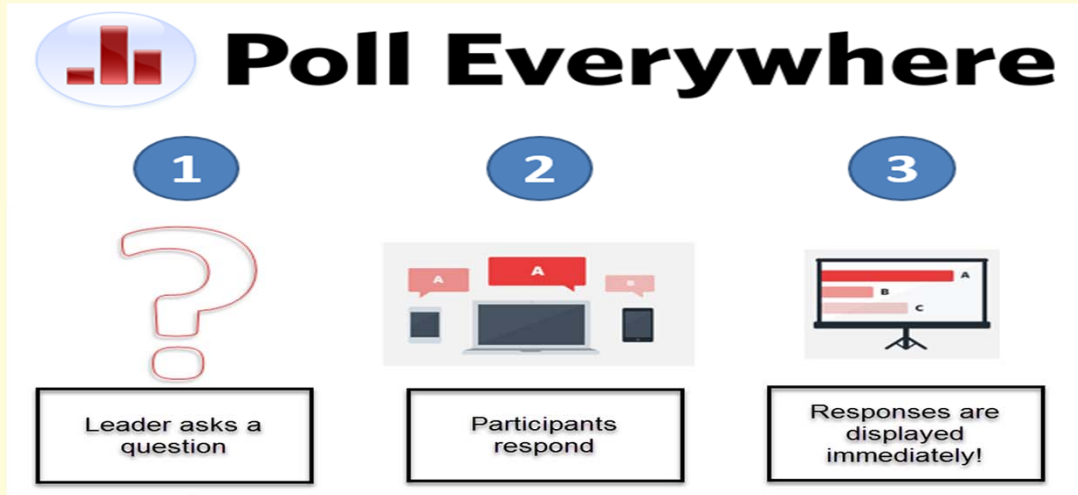
2

KEY POINTS

My Notes



## Participating with Poll Everywhere



3

### 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.

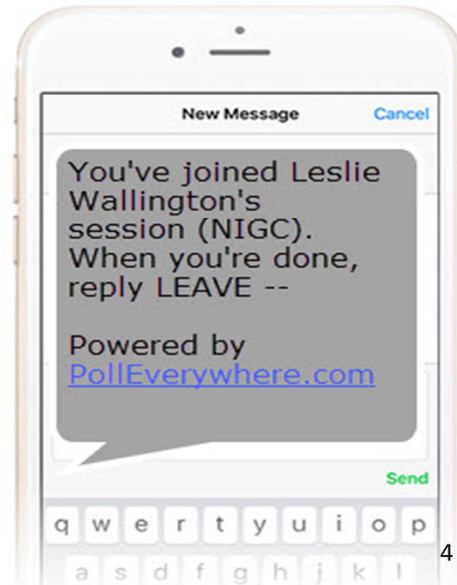
### My Notes

# Participant Guide: IT-113 IT Basics



## Response from Poll Everywhere

1. You will receive a text message confirming that you are in the polling session.
2. Do **NOT** select the [PollEverywhere.com](http://PollEverywhere.com) link.
3. Now you can enter your response to the poll as a text message.



### 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.

### My Notes

# Participant Guide: IT-113 IT Basics



## 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



### KEY POINTS

We're going to have a practice poll question so you get used to using Poll Everywhere.

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

### My Notes



# Participant Guide: IT-113 IT Basics

How did you travel to the conference?

A. Plane

B. Train

C. Car

Foot/Bicycle

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0%

## KEY POINTS

Poll Title: **How did you travel to the conference?**

[https://www.polleverywhere.com/multiple\\_choice\\_polls/yldbms0zVYqpf n5](https://www.polleverywhere.com/multiple_choice_polls/yldbms0zVYqpf n5)

## My Notes

# Participant Guide: IT-113 IT Basics



**How would you rate your IT experience level in a Casino environment?**

Low



Medium

High

Start the presentation to see live content. Still no live content? Install the app or get help at [PollEv.com/app](https://www.poll Everywhere.com/app)

## KEY POINTS

Poll Title: **How would you rate your IT experience level in a Casino environment?**

[https://www.polleverywhere.com/multiple\\_choice\\_polls/EhU9Jx1JIRA08XR](https://www.polleverywhere.com/multiple_choice_polls/EhU9Jx1JIRA08XR)

## My Notes



# Participant Guide: IT-113 IT Basics



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

Low  
Medium  
High

Start the presentation to see live content. Still no live content? Install the app or get help at [PollEv.com/app](https://www.poll Everywhere.com/app)

## 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](https://www.polleverywhere.com/multiple_choice_polls/FtHi407GEQSVUIG)

## My Notes





## IT Basics - Overview

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



KEY POINTS

My Notes

# Participant Guide: IT-113 IT Basics



## IT Basics

EGM

TITO

RNG

SMIB

MICS

Paytable

System  
Verification

CMS

Remote  
Access

Sunset  
Provision

TICS

### 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.
11. **Sunset Provision** – Requiring systems manufactured before 2008 to either be compliant with all 547 standards or be removed from the gaming floor.

### My Notes







## Sunset Provision

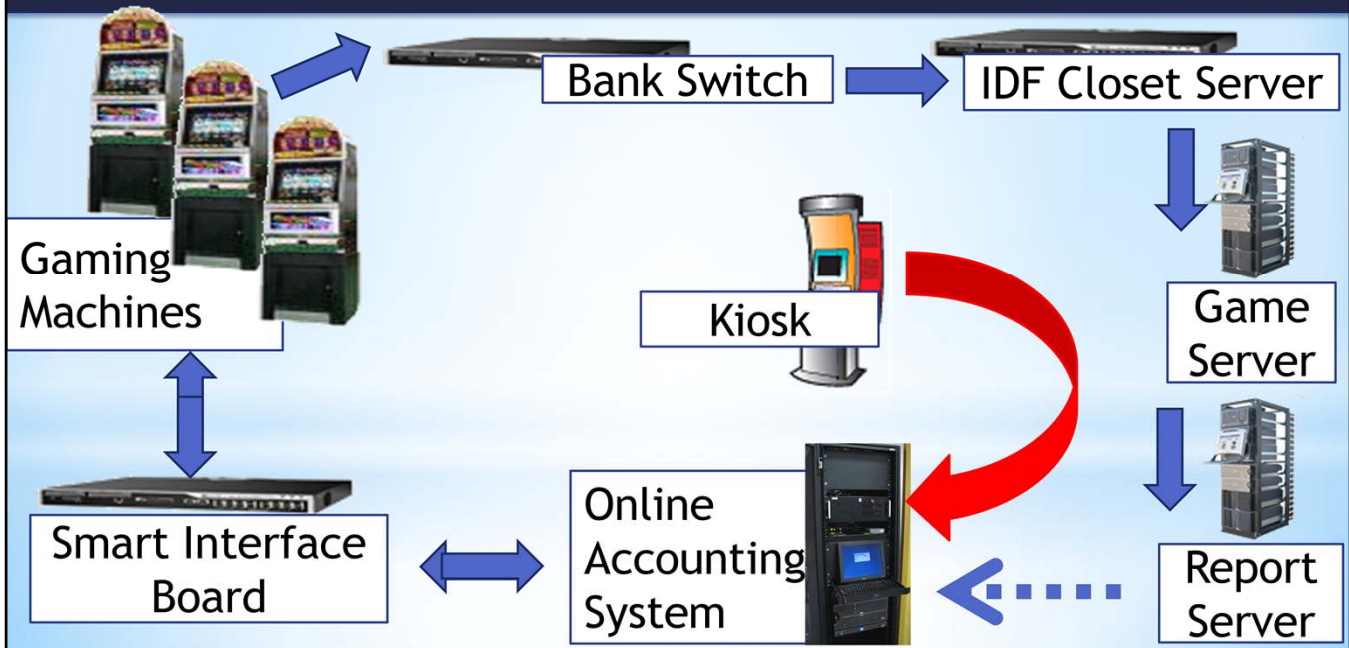
- Removal of the November 10, 2018 sunset for systems manufactured before November 10, 2008 that have not already been made fully compliant with part 547 (2008 systems);
- Requires tribes to conduct an annual review of 2008 Systems to determine whether such systems may be approved pursuant to the standards for newer systems; and
- Requires all system modifications be submitted to a testing laboratory for testing to the standards for newer systems and that Tribal Gaming Regulatory Authorities may approve modifications that either advance or maintain system compliance.

KEY POINTS

My Notes



## Class II Gaming System



### KEY POINTS

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

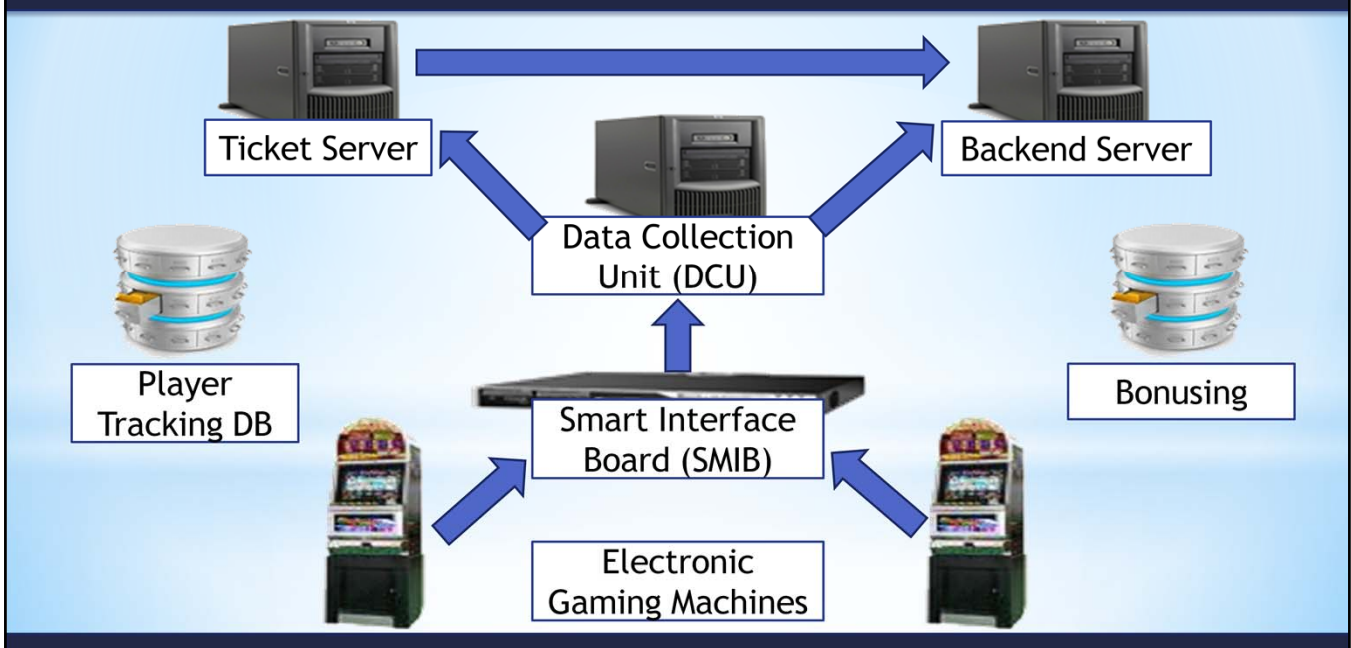
IDF closet switch: Intermediate distribution frame is a room (closet) which contains network equipment.

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.

### My Notes



# Class III Gaming System



KEY POINTS

My Notes





## 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
2. You will be doing one of the following (the instructor will make assignments during class)
3. Present your explanation or definition to the class.

### My Notes



## Activity #2

### Hands On Activity



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

**Group Work**

**TIME: 15 minutes**

**My Notes**



# Participant Guide: IT-113 IT Basics



## 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**

**My Notes**



# Participant Guide: IT-113 IT Basics

## Course Eval IT-113 IT Basics

When survey is active, respond at [PolleEv.com/nigc](https://www.polleverywhere.com/nigc)

0 surveys done

0 surveys underway

Start the presentation to see live content. Still no live content? Install the app or get help at [PolleEv.com/app](https://www.polleverywhere.com/app)

### KEY POINTS

Poll Title: Course Eval IT-113 IT Basics

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

### My Notes

## IT-113 IT Basics Glossary

Term	Definition
<b>Action</b>	The total amount of money bet in a specific period of time.
<b>Arm</b>	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.
<b>Bank</b>	This is used in reference to a row of gaming machines and/or electronic player interface (slot machine) in an establishment.
<b>Bars</b>	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.
<b>Bonus</b>	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.
<b>Bonus Game</b>	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.
<b>Bonus Multiplier Slots</b>	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.
<b>Bonus Video Slots:</b>	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.
<b>Call Attendant</b>	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
<b>Candle</b>	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.
<b>Carousel</b>	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.
<b>Certified</b>	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."
<b>Class II game characteristics</b>	<p>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.</p> <p>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.</p> <p>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.</p> <p>All players play from the same set of numbers as the numbers are announced.</p>
<b>Class III game characteristics</b>	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.
<b>Coin hopper</b>	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.)
<b>Coin Size</b>	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

<b>Term</b>	<b>Definition</b>
<b>Coin-Free Play</b>	Gaming machines and/or electronic player interface (slot machine) play that involves using printed tickets or credit tokens instead of coins.
<b>Coin-In</b>	Refers to the total amount of money a player puts into a gaming machines and/or electronic player interface (slot machine).
<b>Comps</b>	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.
<b>Control (Main) Program</b>	The control program (software that operates the gaming device’s functions such as metering, RNG, control of peripherals, e.g. bill acceptor)
<b>Credit</b>	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.
<b>Credit meter</b>	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.
<b>Double Machines</b>	These machines pay double or triple if winning combinations of certain symbols line up.
<b>Drop Bucket</b>	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).
<b>Drop bucket or drop box</b>	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.
<b>EGM</b>	Stands for "Electronic Gaming Machine" and is often referred to by initials.

## IT-113 IT Basics Glossary

Term	Definition
<b>Flat-Top</b>	“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.
<b>Fraud</b>	<p>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).</p> <p>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.</p>
<b>Hand Pay</b>	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.
<b>Hard Count</b>	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.
<b>Hit</b>	Any winning combination of symbols on the pay line.
<b>Hit Frequency</b>	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
<b>Hold and Re-spin</b>	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.
<b>Hold Percentage</b>	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.
<b>Hopper</b>	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.
<b>House</b>	Another term for casino. Casino literally translates as house in Italian.
<b>House Edge</b>	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.
<b>Jackpot</b>	A gaming machines and/or electronic player interface (slot machine)'s highest payout or can references the top prize in any gambling game.
<b>Linked machines</b>	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.
<b>Load</b>	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).
<b>Loose Machine</b>	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.
<b>Low Level</b>	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.
<b>Max Bet</b>	The maximum amount a player can bet on one spin.

## IT-113 IT Basics Glossary

Term	Definition
<b>MEAL book (Machine entry authorization log)</b>	A log of the employee's entries into the machine.
<b>Mechanical Slots</b>	This refers to the traditional gaming machines and/or electronic player interface (slot machine) that operate with mechanical reels.
<b>MODIFY (AP)</b>	A status used to classify a product that has been modified from its' previous version, which may include: <ol style="list-style-type: none"> <li>1. Manufacturer name change;</li> <li>2. Future implementation of new technology;</li> <li>3. Additional support for new peripheral equipment (Bill Validator, Printer).</li> </ol>
<b>Multiline /Multi-line</b>	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.
<b>Multiplier</b>	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.
<b>NON-MANDATORY UPGRADE (NU)</b>	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: <ol style="list-style-type: none"> <li>1. Inconsequential bug fixes which do not constitute a revocation;</li> <li>2. Program enhancements in the form of new features;</li> <li>3. Help screen verbiage clarification which does not constitute a revocation;</li> <li>4. Issues that require a power cycle to restore (inconvenient but not critical).</li> </ol>
<b>Not Approved (NA)</b>	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.
<b>Odds</b>	The probability of an event. Odds are traditionally expressed as a ratio.
<b>Optimal Play</b>	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).
<b>Pay Cycle</b>	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
<b>Pay For Play</b>	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.
<b>Pay Line</b>	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.
<b>Pay Table</b>	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.
<b>Payback</b>	The percentage of winnings a machine will payout in relation to the amount put in, also known as payout percentage.
<b>Payback Percentage</b>	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.
<b>Pay-line:</b>	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.
<b>Personality (Data) Program</b>	The personality program (software that contains data example reel strips, cards, help screens, graphic sequences to be used by main program)
<b>Poker Machine</b>	Also known as "pokie." The name for a gaming machines and/or electronic player interface (slot machine) in Australia.
<b>Progressive Jackpot</b>	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
<b>Progressive Slots</b>	A group of gaming machines and/or electronic player interface (slot machine) linked together to pay one common big jackpot.
<b>Progressive Ticker</b>	Also known as a Progressive Meter. This shows how much a progressive jackpot is worth.
<b>Random Number Generators</b>	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.
<b>Reels</b>	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.
<b>REVOKED (RV)</b>	<p>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:</p> <ol style="list-style-type: none"> <li>1. Game integrity issues;</li> <li>2. Affects accounting/revenue reporting;</li> <li>3. Issues which may prompt a patron dispute;</li> <li>4. Previous version was found to be non-compliant with jurisdictional regulation;</li> <li>5. Malfunctions requiring a RAM Clear;</li> <li>6. Help/Pay screen was incorrect or misleading;</li> <li>7. Loss of data.</li> </ol>
<b>RNG</b>	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.
<b>Rollup</b>	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
<b>Scatter Pay</b>	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.
<b>Short Pay</b>	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.
<b>Signature Slots</b>	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.
<b>Slant Top Slot</b>	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.
<b>Slot Club</b>	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.
<b>Slot Placement</b>	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.
<b>Slot Schedule</b>	This is information posted on the front of slot that discloses what type of slot, denomination, and win amounts possible for each coin played.
<b>Slot Talk</b>	The information traded between players, a good way to improve slots knowledge.
<b>Slot Tournament</b>	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

<b>Term</b>	<b>Definition</b>
<b>Slots</b>	The nickname for gaming machines and/or electronic player interface (slot machine).
<b>Slots Drop</b>	The amount of money that goes through the gaming machines and/or electronic player interface (slot machine).
<b>Stand Up Slot</b>	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.
<b>Stops</b>	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.
<b>Symbols</b>	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.
<b>Take/Pay Cycle</b>	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.
<b>Theoretical Hold Worksheet</b>	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).
<b>Tight Machine</b>	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.
<b>Tilt</b>	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.
<b>Token</b>	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.
<b>Upright</b>	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

<b>Term</b>	<b>Definition</b>
<b>Video Lottery Terminal</b>	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.
<b>Video Gaming machines and/or electronic player interface (slot machine)</b>	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.
<b>Virtual Reel</b>	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.
<b>Volatility</b>	The ratio of size versus frequency of jackpots in a slot game.
<b>Wild Symbol</b>	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

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

## IT-113 IT Basics Glossary

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

## IT-113 IT Basics Glossary

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



## IT-113 IT Basics Glossary

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

# IT 110 - Refining & Enhancing IT TICS

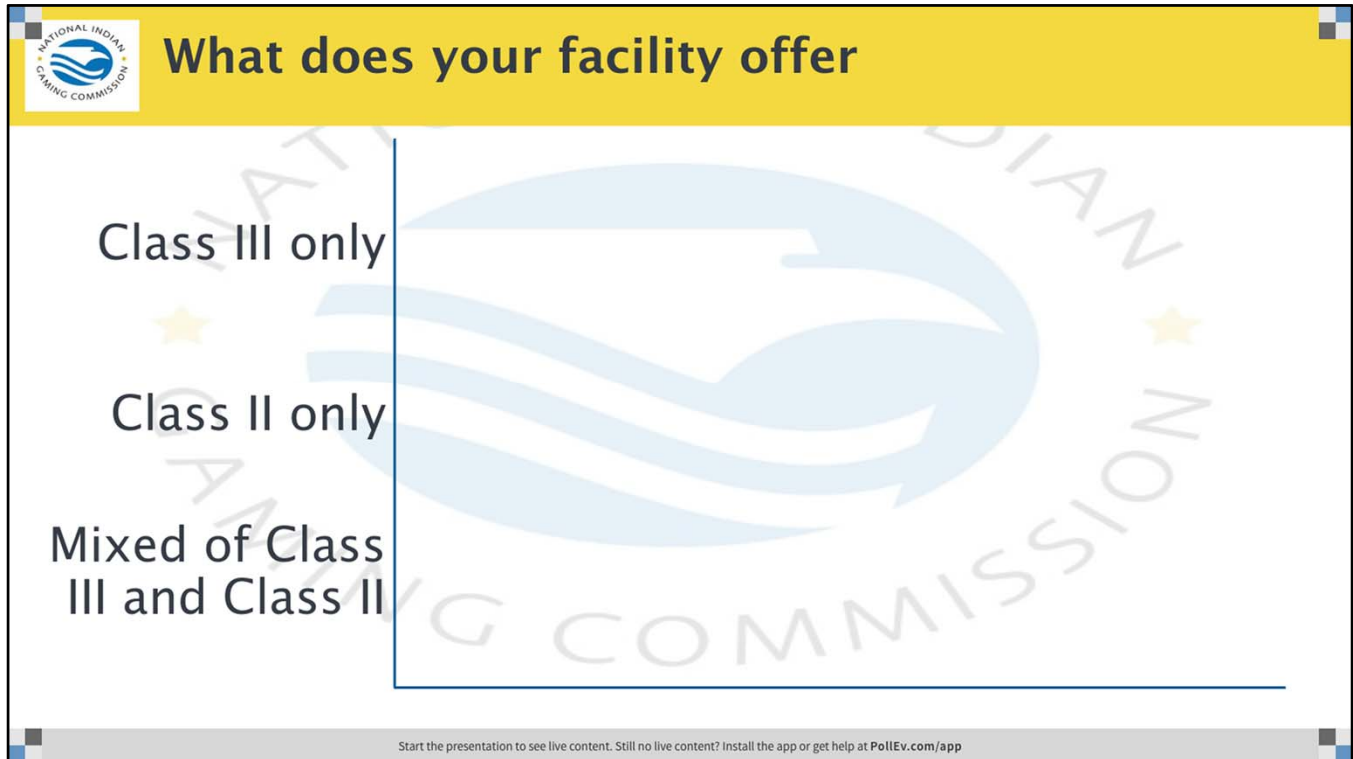


# Refining & Enhancing IT TICS



**Information Technology Division**

**KEY POINTS:**



The image shows a presentation slide for a poll. The slide has a yellow header with the text "What does your facility offer" and the National Indian Gaming Commission logo. The main content area is white and contains three options: "Class III only", "Class II only", and "Mixed of Class III and Class II". A large, faint watermark of the National Indian Gaming Commission logo is visible in the background. At the bottom of the slide, there is a small text box that reads: "Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app".

**What does your facility offer**

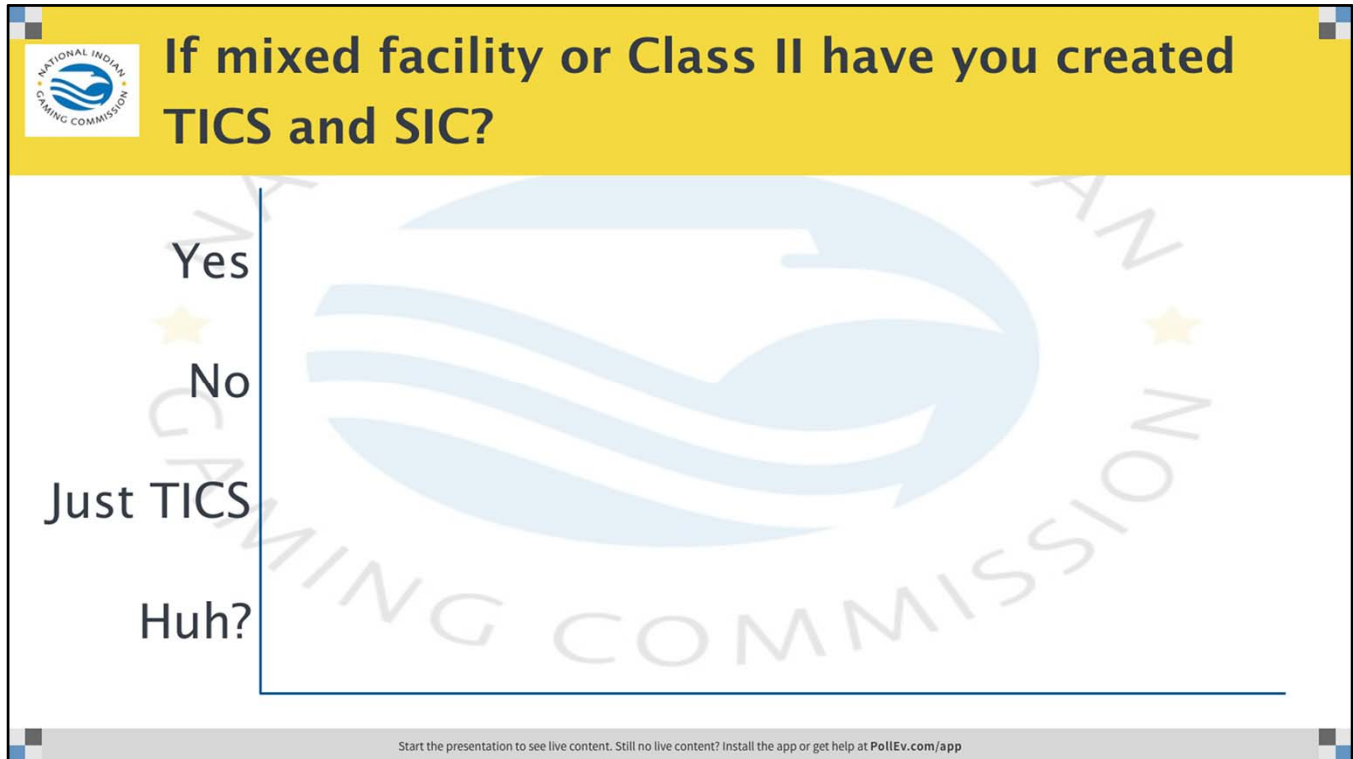
- Class III only
- Class II only
- Mixed of Class III and Class II

Start the presentation to see live content. Still no live content? Install the app or get help at [PollEv.com/app](https://www.polleverywhere.com/app)

## KEY POINTS:

Poll Title: **What does your facility offer?**

[https://www.polleverywhere.com/multiple\\_choice\\_polls/NNFvAQgmzJeMpBw](https://www.polleverywhere.com/multiple_choice_polls/NNFvAQgmzJeMpBw)



**NATIONAL INDIAN GAMING COMMISSION**

**If mixed facility or Class II have you created TICS and SIC?**

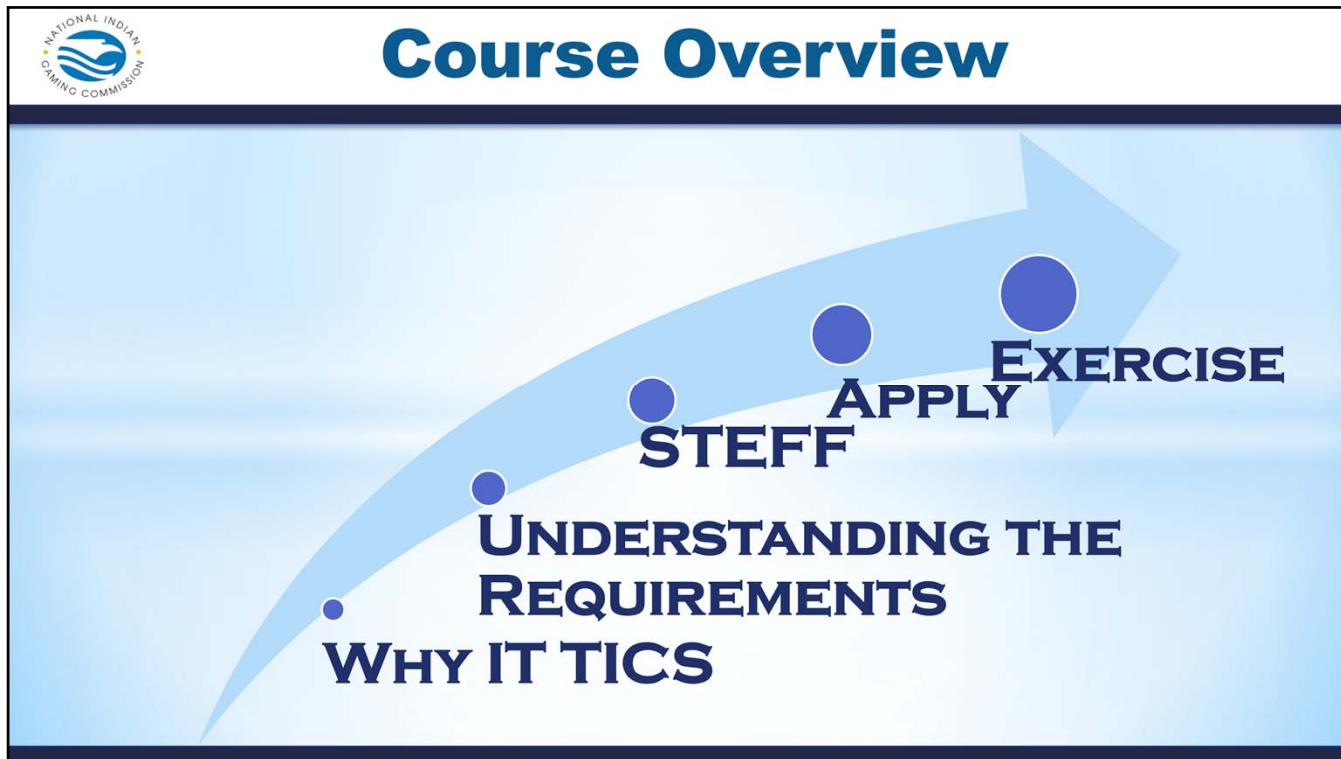
- Yes
- No
- Just TICS
- Huh?

Start the presentation to see live content. Still no live content? Install the app or get help at [PolleEv.com/app](https://www.polleverywhere.com/app)

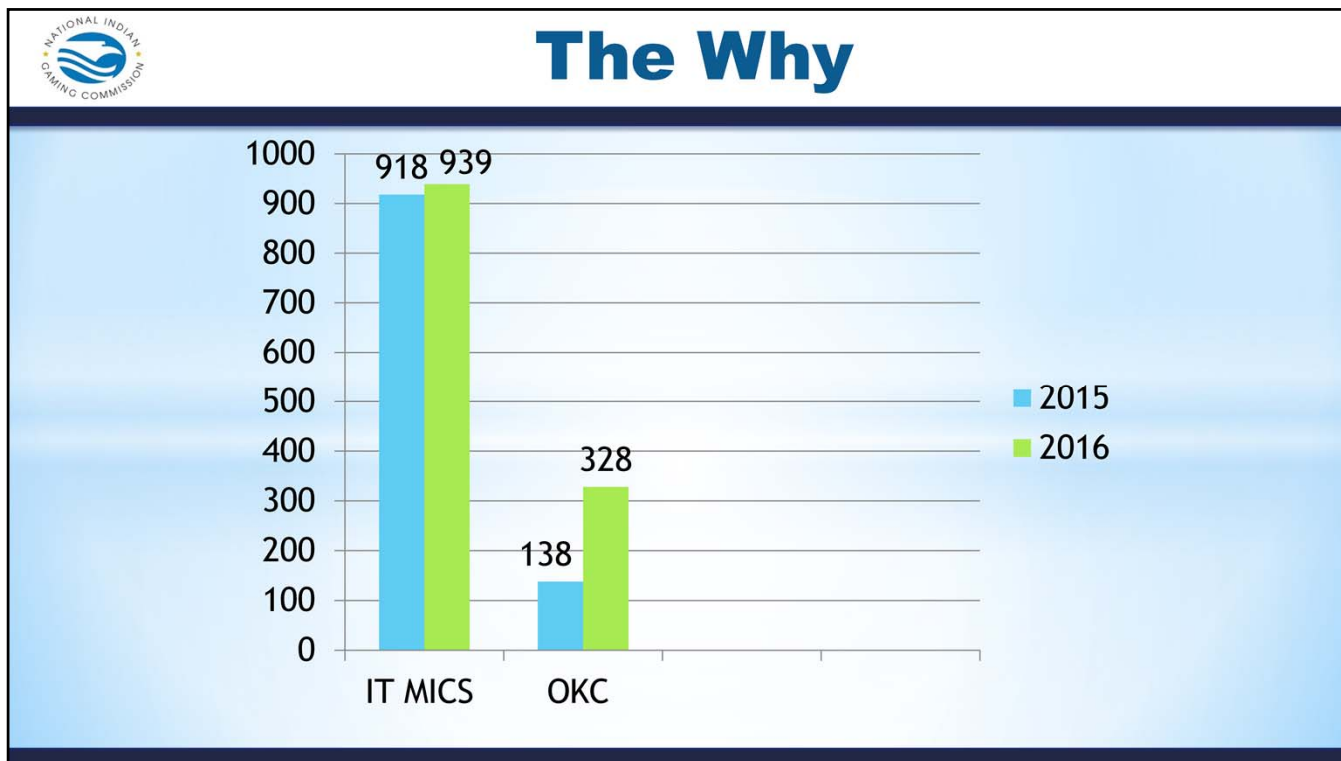
## KEY POINTS:

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

[https://www.polleverywhere.com/multiple\\_choice\\_polls/GFJu2NGRQGmiFI3](https://www.polleverywhere.com/multiple_choice_polls/GFJu2NGRQGmiFI3)



**KEY POINTS:**



**KEY POINTS:**



## 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:





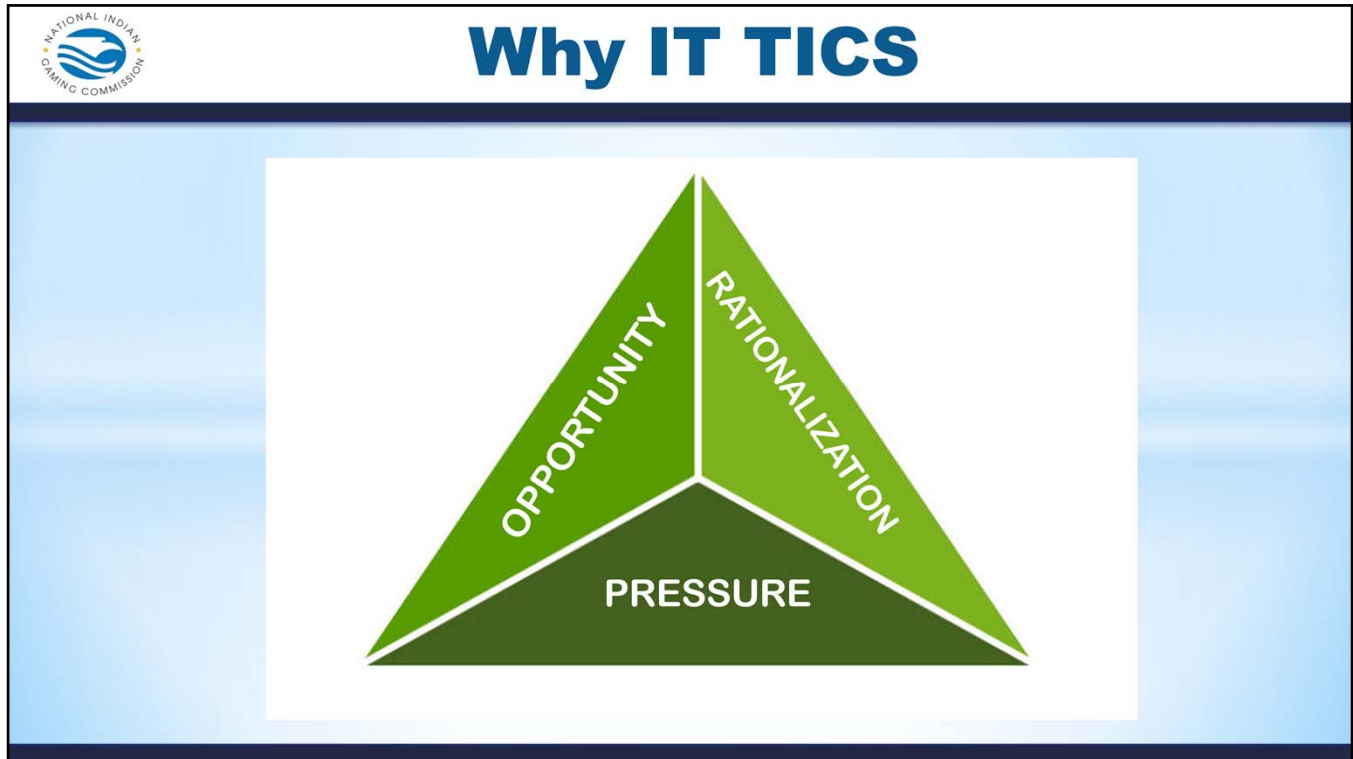
## 543.20(i)(2)

**(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:**



## KEY POINTS

- Internal controls provide reasonable assurances for asset protection, risk mitigation, and reduction in opportunities.



## 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?



## Language - Internal Control Standards

**TRIBAL**

**TICS**

Controls Must Be  
Established

**SYSTEM**

**SICS**

And Procedures  
Implemented to  
ensure adequate...

PRESS

**KEY POINTS:**



## 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?**

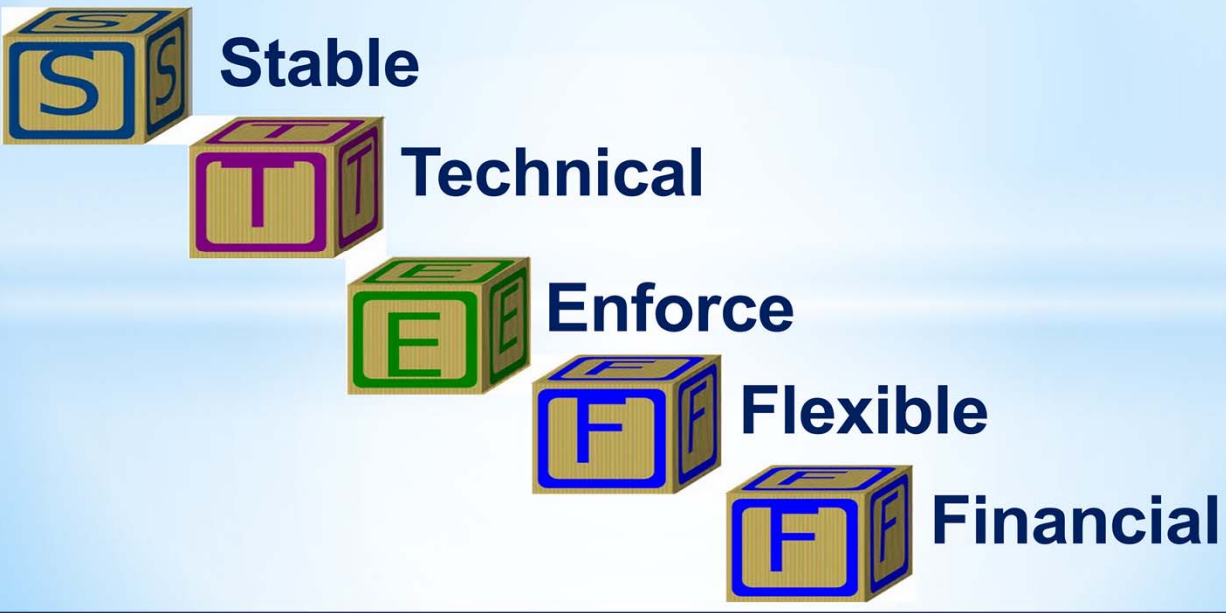
**-and-**

**Why or Why Not?**





## Building Blocks



**S** Stable

**T** Technical

**E** Enforce

**F** Flexible

**F** Financial

KEY POINTS:



## Stable

### IT TICS should:

- Promote a regulatory environment
- Outcome focused

### Accomplished by:

- Employing individuals with requisite IT experience with
- In-depth knowledge of IT systems



### KEY POINTS:





## Technical

### IT TICS should provide:

- Proper technical intelligence for IT TIC enhancement and
- Fostering objective, and transparent procedures

**Greater Transparency  
&  
Increased Accountability**



### KEY POINTS:



## Enforcement

### IT TICS should contain:

- Consistency
- Execution
- Governance
- Independence



### KEY POINTS:



## Flexible

### Sufficient and malleable TICS

- Respond promptly to technical changes
- Emerging IT threats



#### KEY POINTS:



## Financial

### TICS should

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



### KEY POINTS:



## The MICS

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



**KEY POINTS:**



## 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:

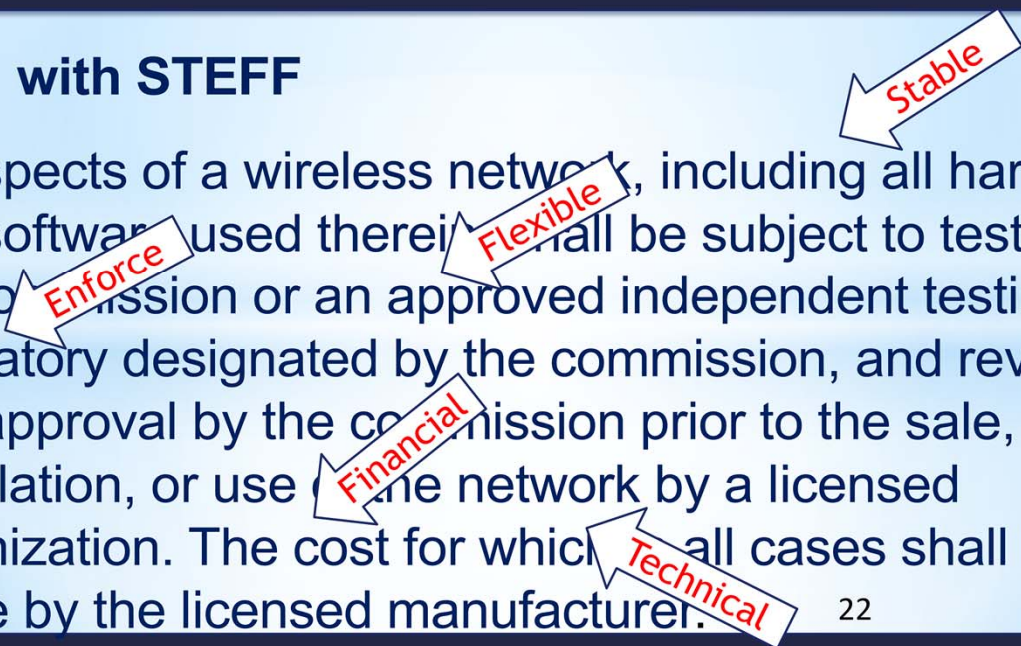
(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;



# 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 POINTS:





 **Are you responsible for the creation, review, or enforcement of your TICS/SICS**

Yes  
No  
I don't know

Start the presentation to see live content. Still no live content? Install the app or get help at [PollEv.com/app](https://www.polleverywhere.com/app)

**KEY POINTS:**

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

[https://www.polleverywhere.com/multiple\\_choice\\_polls/CEjhhc4JyBOPAax](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

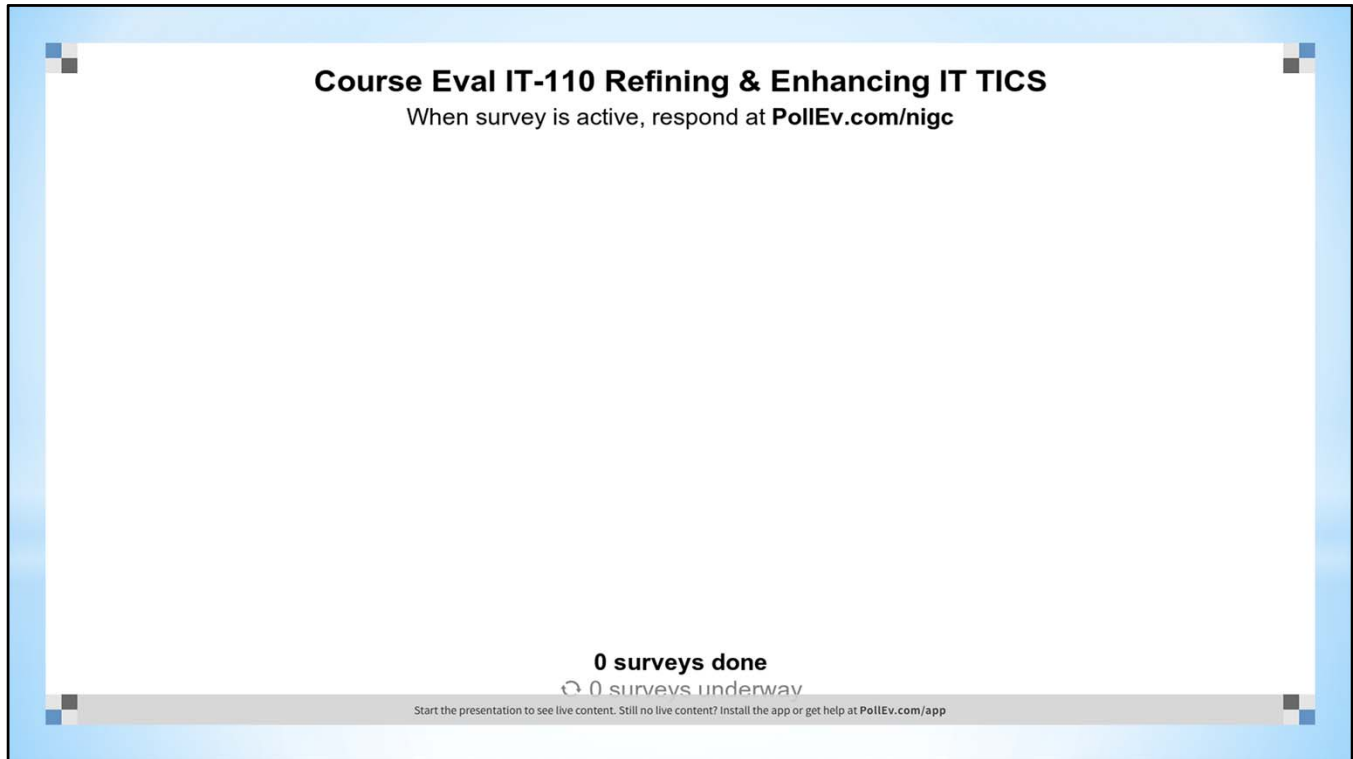
- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciated and allow us to improve your experience



KEY POINTS:

# IT-110 Refining & Enhancing Your IT TICS Course Participant Guide

---



---

## KEY POINTS:

Poll Title: **Course Eval IT-110 Refining & Enhancing IT TICS**

<https://www.polleverywhere.com/surveys/AqxS7Ac6x>

# 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



### Auditing 543.20



Information Technology Division

---

---

---

---

---

---

---

---

### 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

---

---

---

---

---

---

---

---

### What to Expect

- Software Downloads - CFR543.20k
- Verifying Downloads - CFR543.20l
- Installation and/or modifications - CFR543.20g
- Incident monitoring and reporting - CFR543.20i

---

---

---

---

---

---

---

---



---

---

---

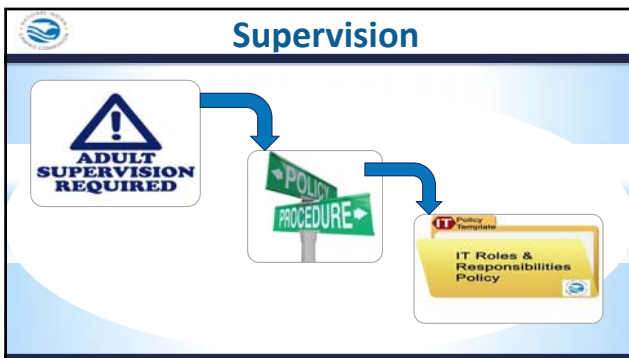
---

---

---

---

---



---

---

---

---

---

---

---

---

**Exercise 1 - Handout #1**

On Handout #1 - fill in the supervision hierarchy from top to bottom.  
(Note: you have more job titles than spaces)

---

---

---

---

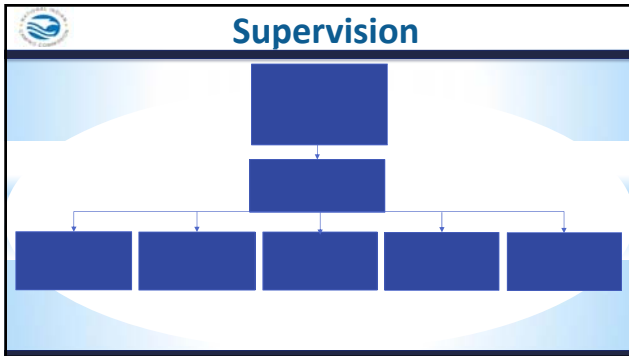
---

---

---

---





---

---

---

---

---

---

---

**Class II Gaming Systems Logical and Physical Controls**

**Importance of:**

- Tribal Internal Controls or (TICS)
- System of Internal Controls or (SICS)

A Venn diagram with four overlapping circles labeled "Threat", "Asset", "Vulnerability", and "Risk". A hand is shown pointing to the intersection of "Threat" and "Asset".

---

---

---

---

---

---

---

**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?

5

---

---


---

---

---

---

---

 **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?

5

---

---

---


---


---

---

---

---

 **Physical Security**



Physical Access

Access History / Access Audit

Data & Hardware Separation

Which Personnel Have Access

---

---

---


---

---

---


---

---

 **Ask Yourself**

1. Are the policy and procedures in place?

2. Who is responsible or has access?



4

---

---

---

---

---

---


---

---

**Ask Yourself**

**3. What group or who is recording and why?**

**4. Should that person be in the area?**



4

---

---

---

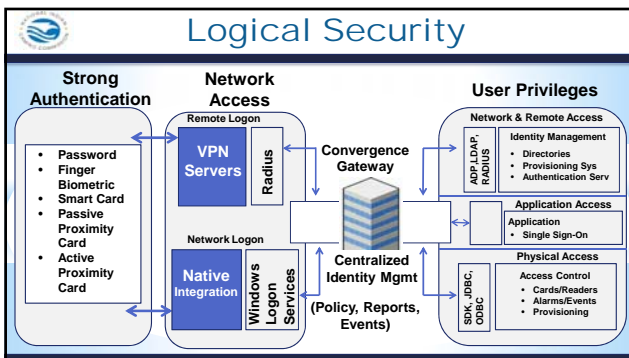
---

---

---

---

---




---

---

---

---

---

---

---

---

**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?**

8

---

---

---


---

---

---

---

---

 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?

8

---

---

---

---

---

---

---

 Exercise #2 - Handout 2



**Handout 2**

---

---


---

---

---

---

---

 INSTRUCTIONS

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

---

---

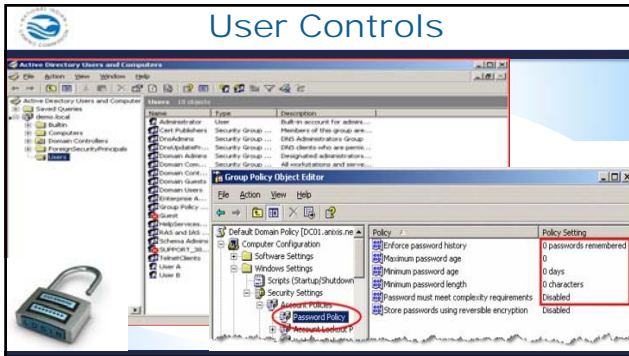
---

---

---

---

---




---

---

---

---

---

---

---

---

### 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?

---

---

---

---

---

---

---

---

### Passwords

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

00000000000000000000 UNCOMMON (NON-GIBBERISH) SINGLE WORD Troub4dor & 3 CAPS? COMMON SUBSTITUTIONS NUMERALS PUNCTUATION <small>(Why don't you try a password like 'Tr0ub4dor&amp;3' to see how it fares?)</small>	~26 BITS OF ENTROPY 2 <sup>26</sup> = 3 DAYS AT 1000 GUESSES/SEC. (Assuming you can guess a new password every 10 seconds and you have a 1000-guess-per-second limit.) DIFFICULTY TO GUESS: EASY
correct horse battery staple FOUR RANDOM COMMON WORDS	~41 BITS OF ENTROPY 2 <sup>41</sup> = 530 YEARS AT 1000 GUESSES/SEC. DIFFICULTY TO GUESS: HARD

Source: <https://kkcd.com/936/>

---

---

---

---

---

---

---

---




---

---

---

---

---

---

---

---

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	VendorName 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	VendorName 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	VendorName of individual performing work	Terminal Services 1h 2m 41s

---

---

---

---

---

---


---

---

**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?




---

---

---


---

---


---

---

---

 **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?

3

---

---

---

---

---

---

---

---

 **Exercise 3 – Handout #3**

**Handout 3**



---

---

---


---

---

---

---

---

 **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.

---

---

---

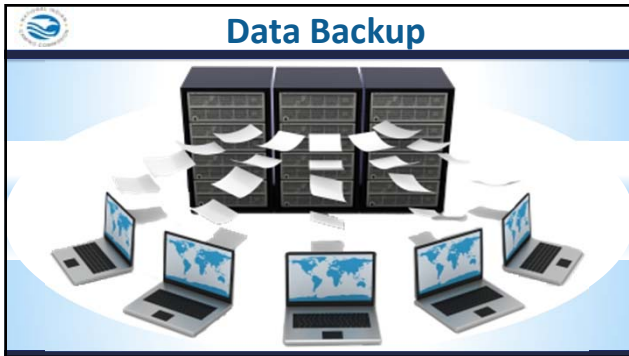
---

---

---

---

---



---

---

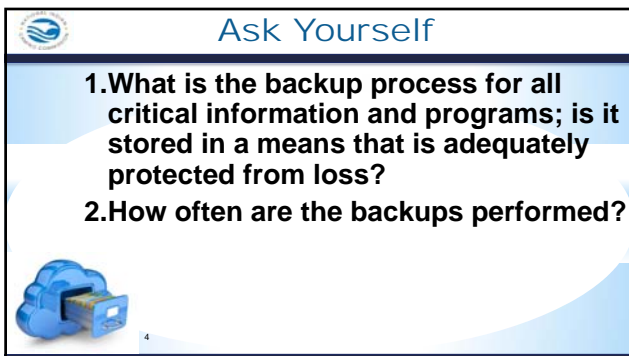
---

---

---

---

---



---

---

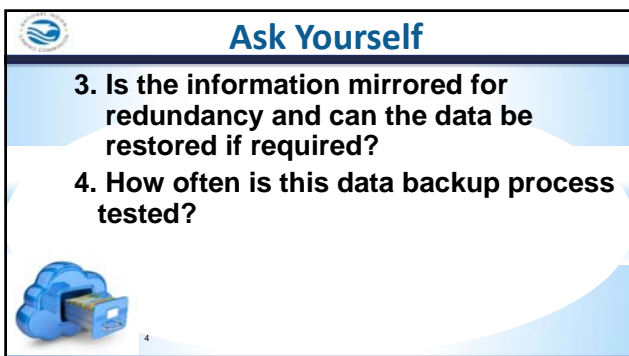
---

---

---

---

---



---

---

---

---

---

---

---



 **Software Downloads**



---

---

---

---

---


---

---

---

 **Verifying Downloads**

*Verified By*



**YOU!**

---

---

---

---

---

---

---

---

 **Installations &/or Modifications**

<p><b>Casino Management System</b></p> 	<p><b>Surveillance</b></p> 
<p><b>Hotel Shops</b></p> 	<p><b>Hospitality</b></p> 

---

---

---


---

---

---


---

---

 **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?



3

---

---

---


---

---


---

---

---

 **Ask Yourself**

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



3

---

---

---


---

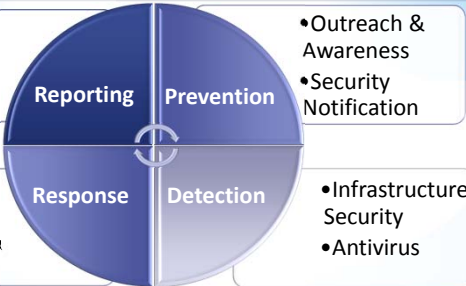
---

---

---

---

 **Incident Monitoring & Reporting**



- Tracking & Referral
- Trending & Analysis
- Forensic Analysis
- Mitigation & Remediation
- Outreach & Awareness
- Security Notification
- Infrastructure Security
- Antivirus

---

---

---


---

---


---

---

---

 **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?



2

---

---

---


---

---

---

---

---

 **Questions**

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

---

---

---

---

---

---

---

---

 **Course Evaluation**

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



---

---

---

---

---

---

---

---

**Knowledge Review - IT-109 Auditing to 543.20**  
When survey is active, respond at [PollEv.com/nigc](http://PollEv.com/nigc)

0 surveys done  
0.0 surveys underway

Start the presentation to get new content, follow the content until the end or go to the PollEv homepage

---

---

---

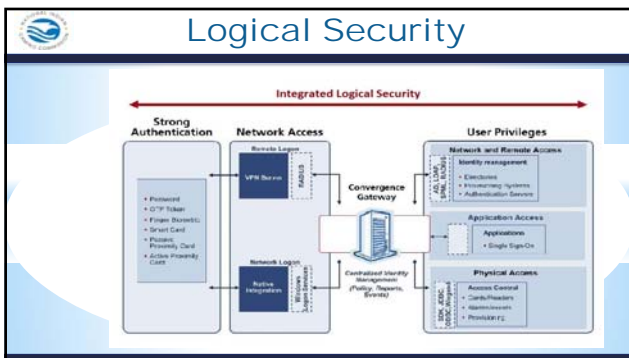
---

---

---

---

---



---

---

---

---

---

---

---

---

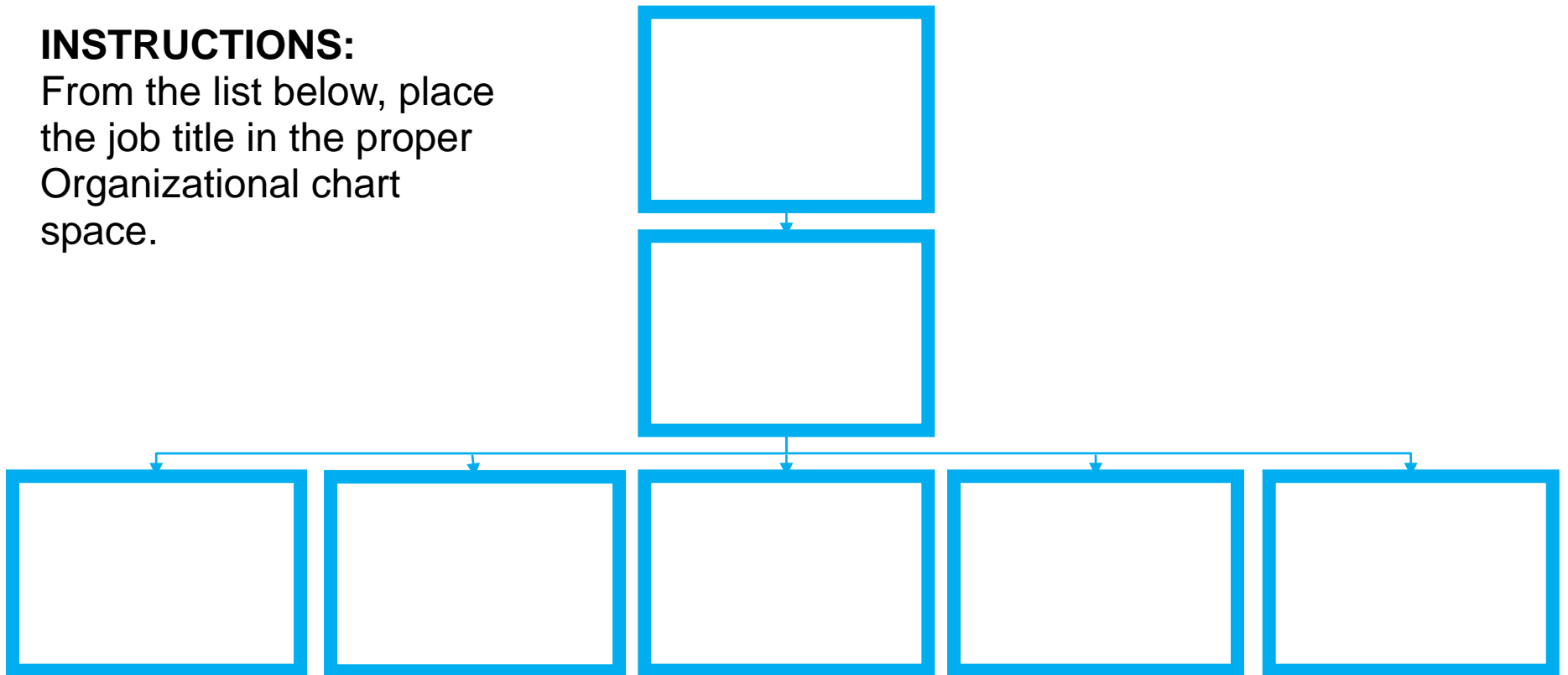
IT 109 -Auditing  
543.20 Handouts



## 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.

<b>Physical security:</b>	<b>Logical security:</b>
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**

## Handout #4 – Exercise 2

### 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:

---

---

---

---

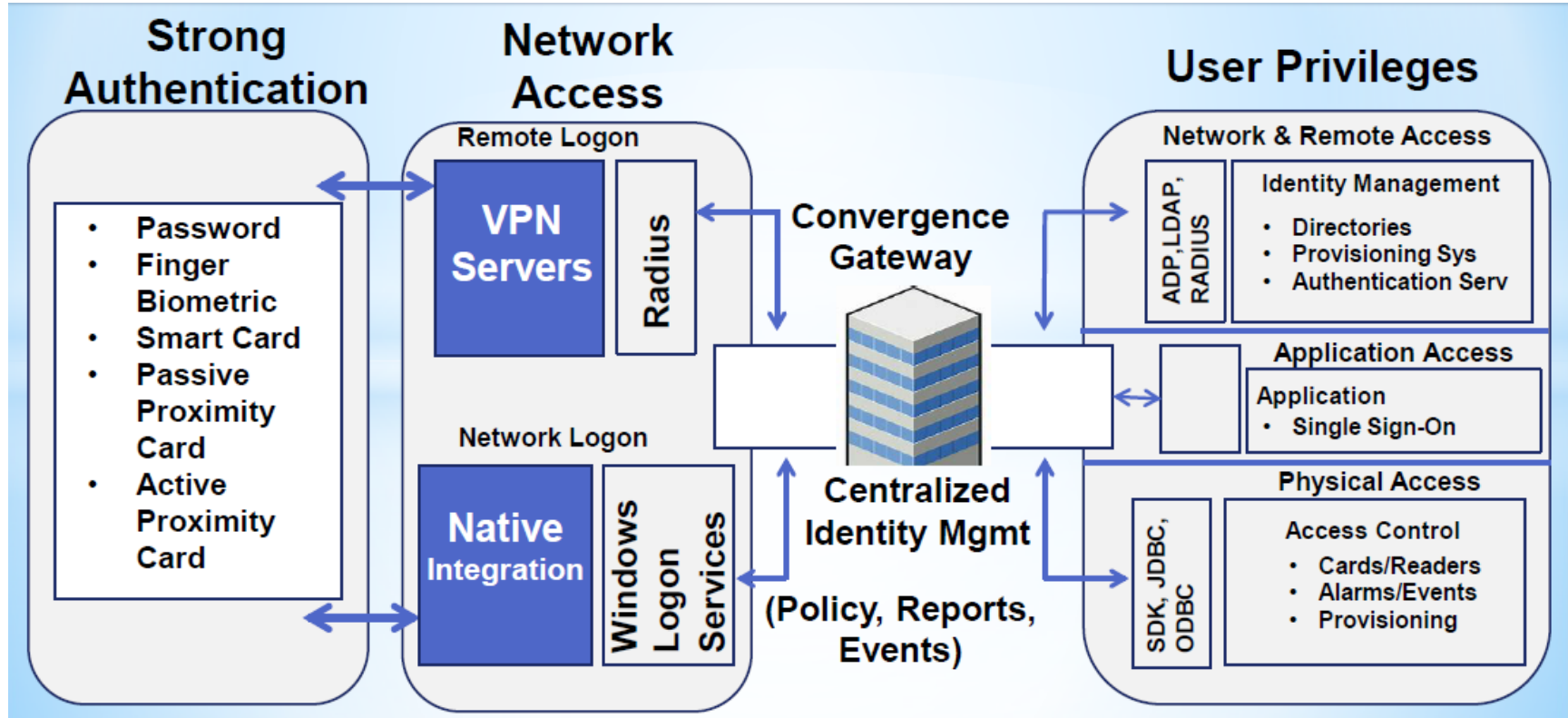
---

---

---

---

# 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 -Systems Verifications & Authentication



### System Verifications & Authentication



Information Technology Division

---

---

---

---

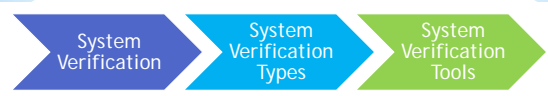
---

---

---

---

### Course Overview



---

---

---

---


---

---

---

---

### System Verification



Internal Testing  
Tested → **Manufacturer Signature**  
c0801a02713b3cdr3407453cg48298

External Testing  
**GLI bmm** **Lab Signature**  
c0801a02713b3cdr3407453cg48298

---

---

---

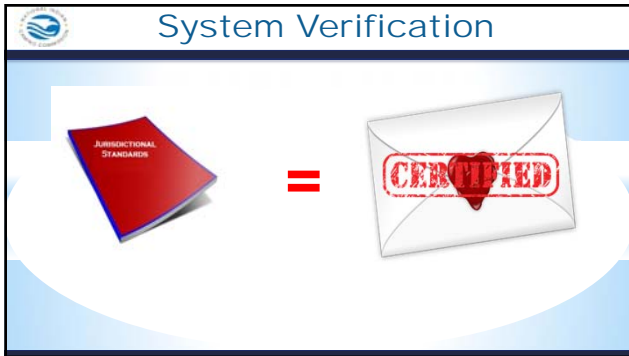
---

---

---

---

---



---

---

---

---

---

---

---

---

System Verification

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

Input	Checksum
Five	1582054465
The red fox jumps over the blue dog	2387213558
The red fox jumps over the blue dog	2043958472
The red fox jumps over the blue dog	332113124
The red fox jumps over the blue dog	1485473564

---

---

---

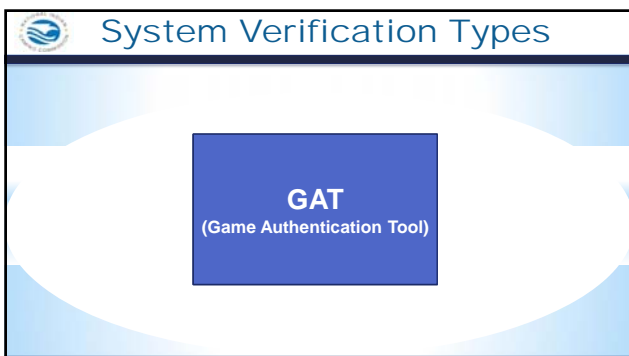
---

---

---

---

---



---

---

---

---

---

---

---

---

 **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.

---

---

---

---

---

---

---

---

 **System Verification Tools**

**GLI** 



---

---

---


---

---

---



---

---

 **System Verification Tools**

**BMM Signatures**

- BMM Signatures was created to provide a tool for the verification of gaming software.

---

---

---

---

---

---

---

---

 System Verification Tools





---

---

---

---

---

---

---

---

 System Verification Tools

CRC



---

---

---

---

---

---

---

---

 System Verification Tools

GLI® 



---

---

---

---

---

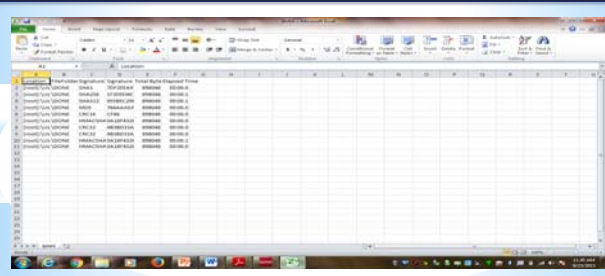
---

---

---



### System Verification Output



The screenshot shows a Windows desktop environment with an Excel spreadsheet open. The spreadsheet contains multiple columns of data, likely representing system verification results. The Windows taskbar is visible at the bottom, showing various application icons.

---

---

---

---

---

---

---

---

### Questions

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

---

---

---

---

---

---

---

---

### Course Evaluation

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



The image shows a hand with the index finger pointing towards three circular smiley face icons. From left to right, they are a yellow neutral face, a green happy face, and a red sad face.

---

---

---

---

---

---

---

---

**Course Eval IT-111 System Verification**  
When survey is active, respond at [PollEv.com/nigc](http://PollEv.com/nigc)

**Start the presentation to activate live content**  
If you see this message in present mode, you are the presenter get help at [PollEv.com/help](http://PollEv.com/help)  
© 2014 SurveyGizmo, Inc.

---

---

---

---

---

---

---

IT 108 -  
Vulnerabilities, Tech  
Exploits, and Cyber  
Defenses



# IT Vulnerabilities, Tech Exploits, and Cyber Defenses



Information Technology Division

---

---

---

---

---

---

---

---

## Overview



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

---

---

---

---

---

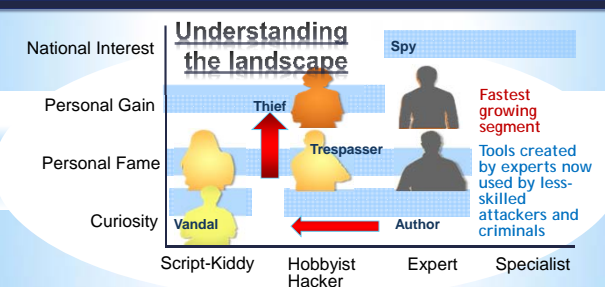
---

---

---

## Setting

**Understanding the landscape**



Motivations: National Interest, Personal Gain, Personal Fame, Curiosity

Roles: Script-Kiddy, Hobbyist Hacker, Expert, Specialist

Activities: Vandal, Thief, Trespasser, Author, Spy

Notes: Fastest growing segment; Tools created by experts now used by less-skilled attackers and criminals

---

---

---

---

---

---

---

---

### 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	2008	26,500,000	government, military	lost / stolen computer
Taobao	2016	20,000,000	retail	hacked
Vodafone	2013	2,000,000	telecoms	inside job

---

---

---

---

---

---

---

---

---

---

### Physical Environment

Shared use

Physical servers

Virtual servers

Printers

Individual use

Desktops / Smartphones / tablets

Network equipment

Managed / Unmanaged

ISPs

WiFi Access points

Audio Visual

IP phones

Signage

Smart Devices

IP Cameras / TV / DVR

MVAC

Internet of things (IoT) devices

\*\*All devices and Oses are susceptible.

---

---

---

---

---

---

---

---

---

---

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique public key RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **Single Copy** of the private key, which will allow you to decrypt the files, located on a secret server on the internet; the server will **destroy** the key after a time specified in this window. After that, **subonly and never will be able** to restore files.

To **obtain** the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click **«Next»** to select the method of payment and the currency.

**Any attempt to restore or damage this software will lead to the immediate destruction of the private key by server.**

Private key will be destroyed on:

13/06/2018 09:42

Time left: 71:59:13

---

---

---

---

---

---

---

---


---

---

### 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

---

---

---

---

---


---

---

---

### Network Attacks

#### SQL Injection



Defenses:

- Run database service account with minimal rights
- Disable commands like xp\_cmdshell
- Suppress all error messages
- Use custom error messages
- Use low privileged account for DB connection
- Filter all client data
- Use only stored procedures to validate user input
- Use SQL Injection Detection tools

---

---

---

---

---

---

---

---

### Malware Defense Techniques

#### Defense best practices

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

---

---

---

---

---

---

---

---

### Activity - Identify the Dangers

Smart TVs    IP cameras    VoIP phones    Printers

Voice recognition software    HVAC    Cable / Satellite    POS

---

---

---

---

---

---

---

---

### Wireless Network Attacks

#### Packet Sniffing / AP impersonation

Types of attacks:

- DHCP Attacks
- ARP Poisoning
- Spoofing / Evil Twin
- DNS Poisoning
- Password Capture
- Wireless pivots

---

---

---

---

---

---

---

---

### Network Hacking Tools

#### Packet Analyzers

---

---

---

---

---

---

---

---

### Activity - Wireshark Demo



---

---

---

---

---

---

---

---

### Protocols Vulnerable to Sniffing

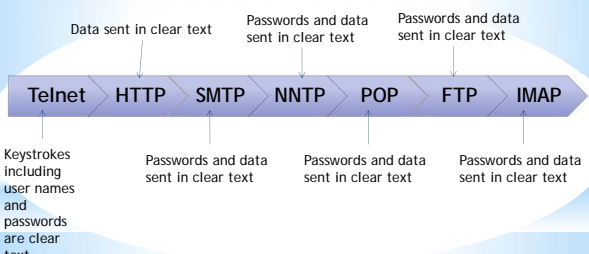


Diagram illustrating protocols vulnerable to sniffing:

- Telnet: Keystrokes including user names and passwords are clear text
- HTTP: Data sent in clear text
- SMTP: Passwords and data sent in clear text
- NNTP: Passwords and data sent in clear text
- POP: Passwords and data sent in clear text
- FTP: Passwords and data sent in clear text
- IMAP: Passwords and data sent in clear text

---

---

---

---

---

---

---

---

### 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!

---

---

---

---

---

---

---


---



**Network Hacking Tools/Methods**

"Password recovery" tools.  
(Aka. Cracking)

- Hashcat
- Cain
- Aircrack-ng




---

---

---

---

---

---

---

---

**Cracking Continued**

**Brute Force**

0001  
0002  
0003  
Test

**Mask attack**

password  
Password  
Password1  
Password1@

**Attack types**

**Dictionary List**

pass  
12345  
omg  
Test

**Combinator**

**Output**

```

passpass
pass12345
passomg
passTest
12345pass
1234512345
12345omg
12345Test
omgpass
omg12345
omgomg
omgTest
Testpass
Test12345
Testomg
TestTest
  
```

---

---

---

---

---

---

---

---

**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.

---

---

---


---

---

---


---

---

 **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

---

---

---


---

---

---

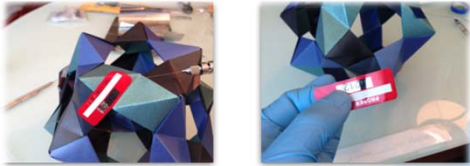
---

---

 **Human Error – Tamper Proof**

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

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



---

---

---


---

---

---

---

---

 **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

---

---

---

---

---

---

---

---

**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)

---

---

---

---

---

---

---

---

---

---

**Human Error-Social Engineering**

### Dumpster Diving / Trashing

Large amounts of information can be collected through company trash, such as:

- company phone books - organizational charts - memos - system
- calendars of meetings - events and vacations - company policy manuals
- printouts of sensitive data or login names and passwords - printouts of source code
- disks and tapes - company letterhead and memo forms - outdated hardware

---

---

---

---

---

---

---

---

---

---

**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

---

---

---

---

---

---

---

---


---

---

### 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



---

---

---

---

---


---

---

---

### 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

---

---

---

---

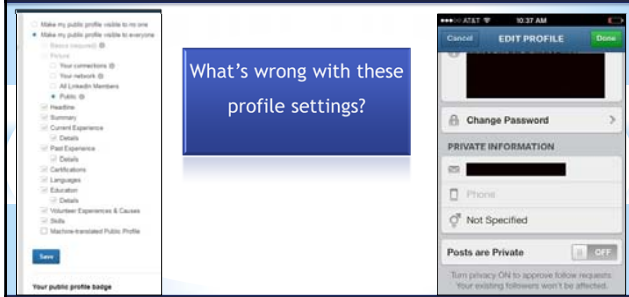
---

---

---

---

### Activity - Identify the Problem(s)



What's wrong with these profile settings?

---

---

---

---

---

---

---

---

### Activity - Identify the Problem(s)

The screenshot shows the 'Privacy Settings and Tools' page on Facebook. The left sidebar lists various settings categories: General, Security and Login, Privacy, Timeline and Tagging, Blocking, Language, Notifications, Mobile, Public Posts, Apps, Ads, Payments, Support Inbox, and Videos. The main content area is titled 'Privacy Settings and Tools' and contains several sections with settings and 'Edit' links:

- Who can see my stuff?**
  - Who can see your future posts? Public Edit
  - Who can see your friends list? Friends Edit
  - Review all your posts and things you're tagged in Use Activity Log
  - Limit the audience for posts you've shared with friends of friends or Public? Limit Past Posts
- Who can contact me?**
  - Who can send you friend requests? Everyone Edit
- Who can look me up?**
  - Who can look you up using the email address you provided? Everyone Edit
  - Who can look you up using the phone number you provided? Everyone Edit
  - Do you want search engines outside of Facebook to link to your profile? Yes Edit

---

---

---

---

---

---

---

---

### Ways to Mitigate IT Threats

The diagram consists of five blue chevron-shaped boxes pointing to the right, each containing a strategy and its sub-points:

- 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**

---

---

---

---

---

---

---

---

### 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.

---

---

---

---

---

---

---

---

**On the Horizon**

# Bitcoin

- Crypto currency
- Peer to peer electronic cash system
- No reserve no backing
- High degree of anonymity
- Code not an ID represents digital signature

- Bitcoin is one particular application of blockchain technology.

- The act of verifying the transactions "the chain" generates new bitcoins for the verifier.

---

---

---

---

---

---

---

---

**On the Horizon**

## Etherium and Smart Contracts

> Ethereum is a usage of blockchain technology. Mining ether cryptocurrency

> Ethereum 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

---

---

---

---

---

---

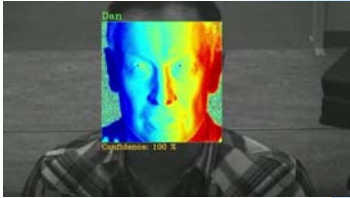
---

---

**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>

---

---

---


---


---

---


---

---

 On the Horizon



RFID scanning  
and cloning



<p><b>Dangers for:</b> Key FOBs HID (Human Interface device)</p>	<p><b>Mainstream:</b> Cheap / portable How-to instructions are plentiful</p>
--	--

---

---

---


---


---

---

---

---

 On the Horizon



Air gapping, Li-Fi and other non-traditional  
data transfer methods and networks

**More common examples:**

- > Air Hopper
- > NSA standard TEMPEST
- > Origins with techniques like Van Eck phreaking ( displaying output from a closed network monitor)

**Can utilize:**

- Acoustic - Air Hopper uses laptop speakers and mic
- Light - LiFi
- Magnetic - monitor radiation
- Seismic
- Thermal
- Radio-frequency
- Physical media

---

---

---

---

---

---

---

---

 On the Horizon

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



---

---

---


---

---

---

---

---

 **Questions**

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

---

---

---

---

---

---

---

---

 **Course Evaluation**

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



---

---

---

---

---

---

---

---

**Course Eval IT-108 IT Threats**  
When survey is active, respond at [PollEv.com/nigc](http://PollEv.com/nigc)

**Start the presentation to activate live content**  
If you see this message in presentation mode, you'll see a video or get help at [PollEv.com/help](http://PollEv.com/help)

---

---

---

---

---

---

---

---



# IT 107 - Gaming Forensics



## Gaming Forensics



Information Technology Division

---

---

---

---

---

---

---

---

## Digital Forensics



---

---

---

---

---

---

---

---

## Course Overview



### WHAT?

- Common Types
- Investigations

### WHY?

- Chain of Custody
- Evidence Gathering

### WHO?

- First Responders
- Gaming Commissions

### HOW?

- Plan of Action
- Collected Evidence

---

---

---

---

---

---

---

---

Has anyone gone through a forensic with ITL?

Yes

No

sure

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at [PUBL.com/help](http://PUBL.com/help)

---

---

---

---

---

---

---

---

Gaming Forensics

- Criminalistics
- Video Analysis
- Accounting

---

---

---

---

---

---

---

---

Gaming Forensics

**LAW**

**ANOTHER JACKPOT MALFUNCTION**

---

---

---


---

---


---

---

---

 **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



---

---

---

---

---

---

---

---

 **Investigative Purpose**

**Public Trust**

MICS 547.5 TGRA chooses ITL for certification 

---

---

---


---

---


---


---

---

 **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)



---

---

---

---


---

---

---

---

Evidence Gathering



WHY?

---

---

---

---

---

---

---

---

Evidence Gathering



MICS 547.13 Program Storage Media

WHY?

---

---

---

---


---

---

---

---

Evidence Gathering



WHY?

---

---

---


---

---

---


---

---

 **First Responders**

Those directly affecting gaming integrity

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



---

---

---

---

---

---

---

---

**Does anyone have a first Responders Team?**

Yes

No

Working on it

Start the presentation to activate live content  
If you see this message in presentation mode, install the add-in or get help at Pdf24.com/app

---

---

---


---

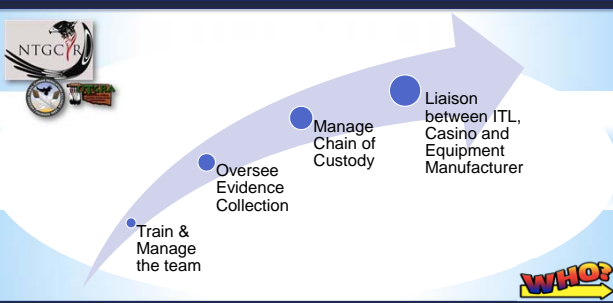
---


---

---


---

 **FRT - Regulators**





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



---

---

---

---

---

---

---

---

FRT - Gaming Operations

The slide features a central white cloud with the text "Report Findings". To the left is a red button labeled "DEPLOY" and a blue button labeled "IDENTIFYING". Below the cloud are three blue boxes: "Inform Personnel", "DO NOT TURN IT OFF, OR ON IF OFF", and "Findings Regulatory Body(s)". A "WHO?" sticker is in the bottom right corner.

Report Findings

WHO?

---

---

---

---

---

---

---

---

FRT - Information Technology

The slide features a central white cloud with the text "Report Findings". The background shows a screenshot of system logs and a network diagram. Text labels include "Backend Sys Logs", "Account System Error Logs", and "Access System Logs". A "WHO?" sticker is in the bottom right corner.

Report Findings

Backend Sys Logs

Account System Error Logs

Access System Logs

MICS 547.3 Responsibility for technology

WHO?

---

---

---

---

---

---

---

---

FRT - Security

The slide features a central white cloud with the text "Report Findings". The background shows a cardboard box with a red "EVIDENCE SEAL" sticker. A "WHO?" sticker is in the bottom right corner.

Report Findings

WHO?

---

---

---


---

---

---

---

---


 FRT - Surveillance

Control  
C  
Cov

Report Findings

Surveillance  
o of  
ection

MICS 543.21 Surveillance



---

---

---


---

---

---

---

---


 FRT - Accounting & Audit

Report Findings

Cashout  
CASHOUT  
CASHOUT  
CASHOUT

Casino  
Management  
System

MICS 547.8(2)(k) Critical Memory gain (i) Accounting data



---

---

---


---

---



---

---

---

 Gaming Commission

As the regulatory body submits information and components for a forensic examination following a thorough investigation and gathering of information and evidence.



---

---

---

---

---

---


---

---



### Plan of Action

- First Responder Team
- Forensic Threshold
- Escalation
- Readiness Training



---

---

---

---

---


---

---

---

### Collected Evidence

Must be secured and stored in a controlled environment



---

---

---

---

---

---


---

---

### 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



---

---

---


---

---

---

---

---

 **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.)?

---

---

---


---

---

---

---

---

 **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

---

---

---


---

---

---

---

---

 **Questions**

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

---

---

---


---

---

---

---

---

 **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

**QUESTIONS**

1- A B C D

2- A B C D

3- A B C D

4- A B C D

5- A B C D

6- A B C D

---

---

---

---

---

---

---

---

**FY2018 RGT Knowledge Review Day 2**  
When survey is active, respond at [PollEv.com/nigc](http://PollEv.com/nigc)

0 surveys done

0.0 surveys answered

Start the presentation to see the content, follow the content, scroll to stop or get help at PollEv.com/help

---

---

---

---

---

---

---

---

 **Course Evaluation**

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

---

---

---

---

---

---

---

---

**Course Eval IT-107 Forensics in Gaming**  
When survey is active, respond at [PollEv.com/nigc](http://PollEv.com/nigc)

**Start the presentation to activate live content**  
If you see this message in present, click back, you will be redirected to get help at [PollEv.com/help](http://PollEv.com/help)  
© 2016 SurveyGizmo, Inc.

---

---

---

---

---

---

---

---