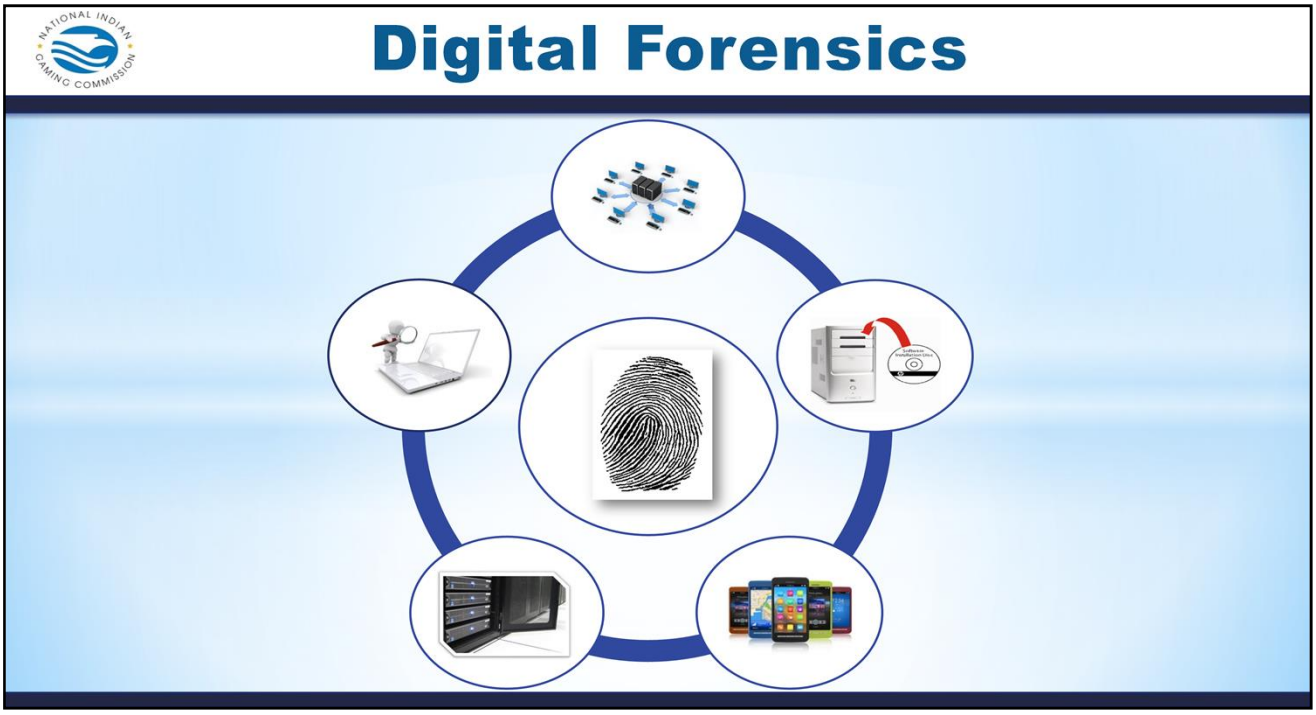
IT-107 Gaming Forensics

Information Technology Division

KEY POINTS



KEY POINTS

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


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

KEY POINTS

KEY POINTS

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

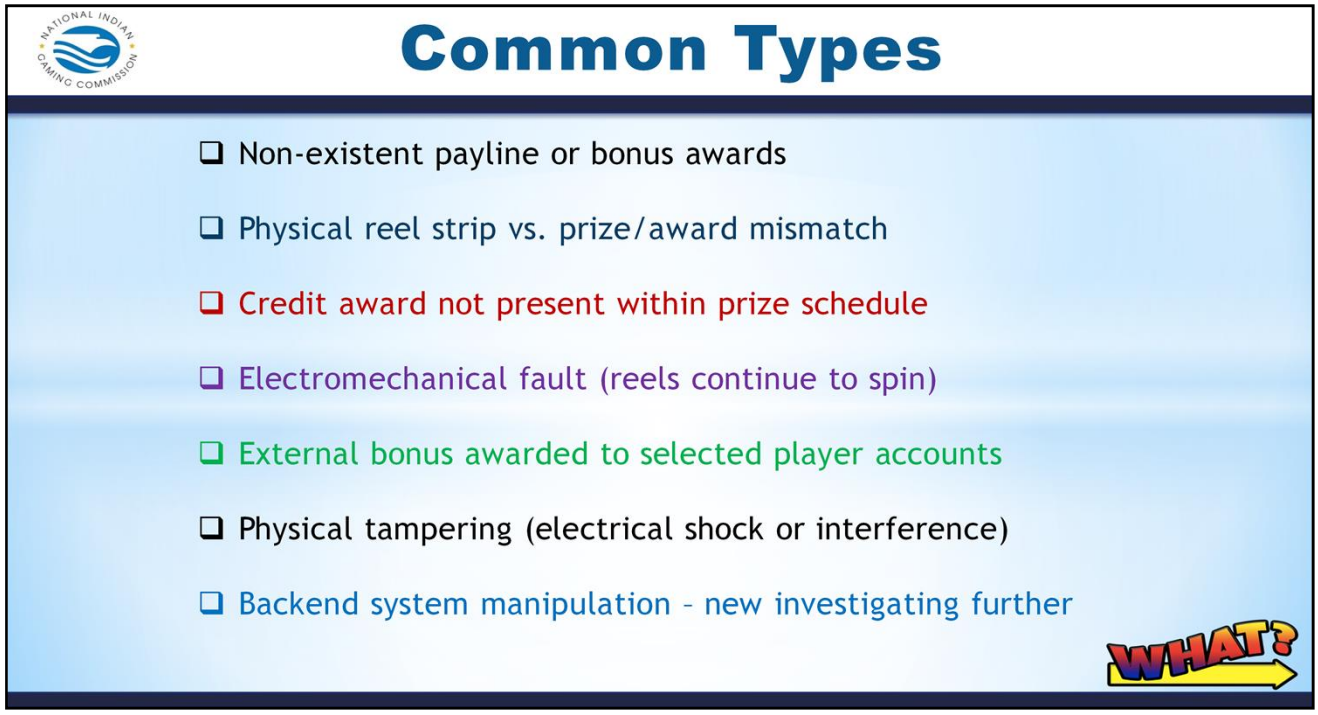
https://www.polleverywhere.com/multiple_choice_polls/TV3tvEM9ndVGHB9

KEY POINTS

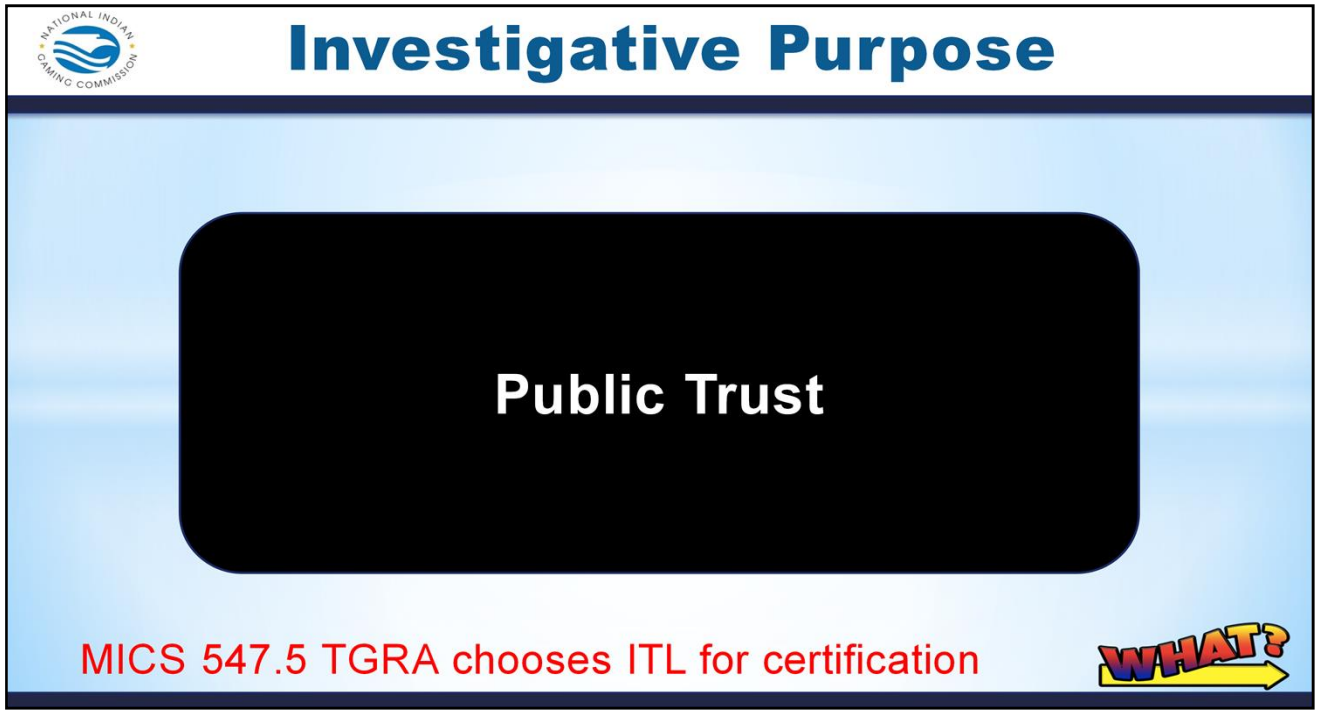
1. Criminalistics are the study and collection of physical evidence at the crime.
2. Video Analysis is the scientific study and collection of video for legal matters.
3. Accounting is the study and analysis of collection of financial evidence.

KEY POINTS

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


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

KEY POINTS



KEY POINTS

Why are forensic investigations and relevant procedures important?

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

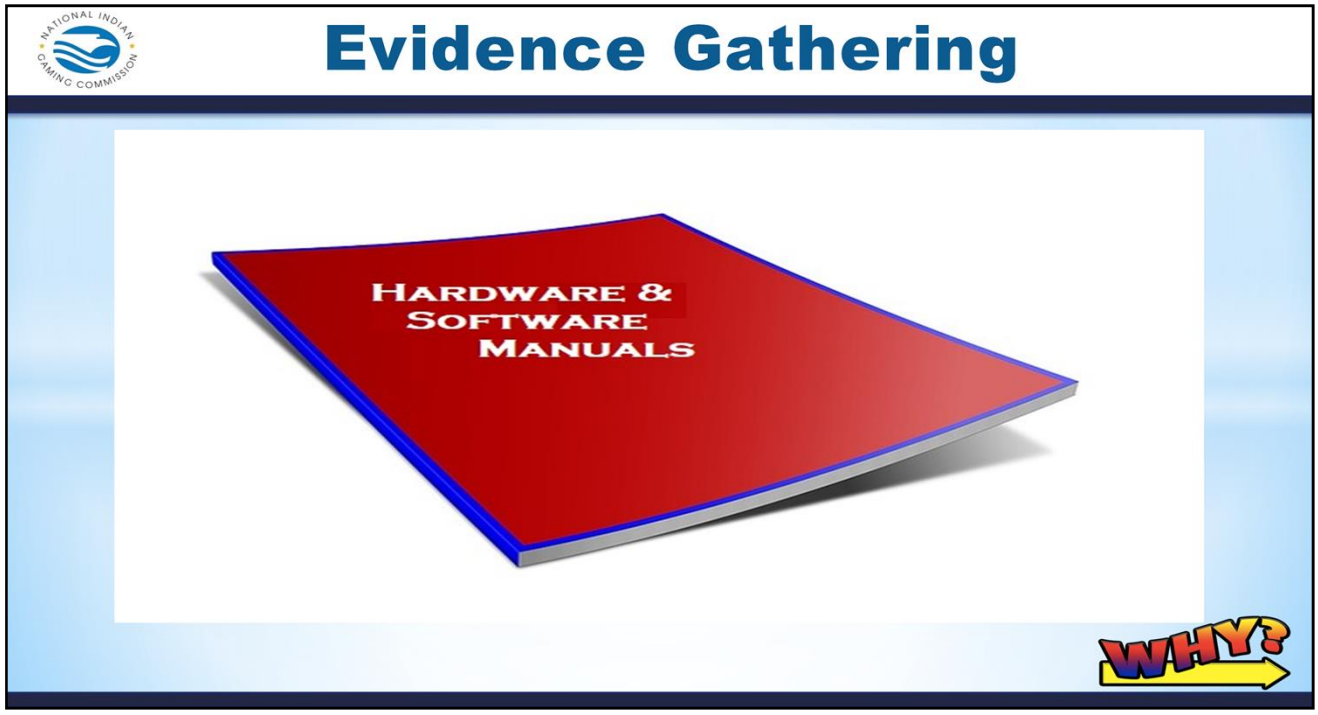
Chain of Custody

Include:

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

KEY POINTS

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



KEY POINTS

Examples of physical/non-electronic evidence include:

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

Examples of physical/non-electronic evidence include:

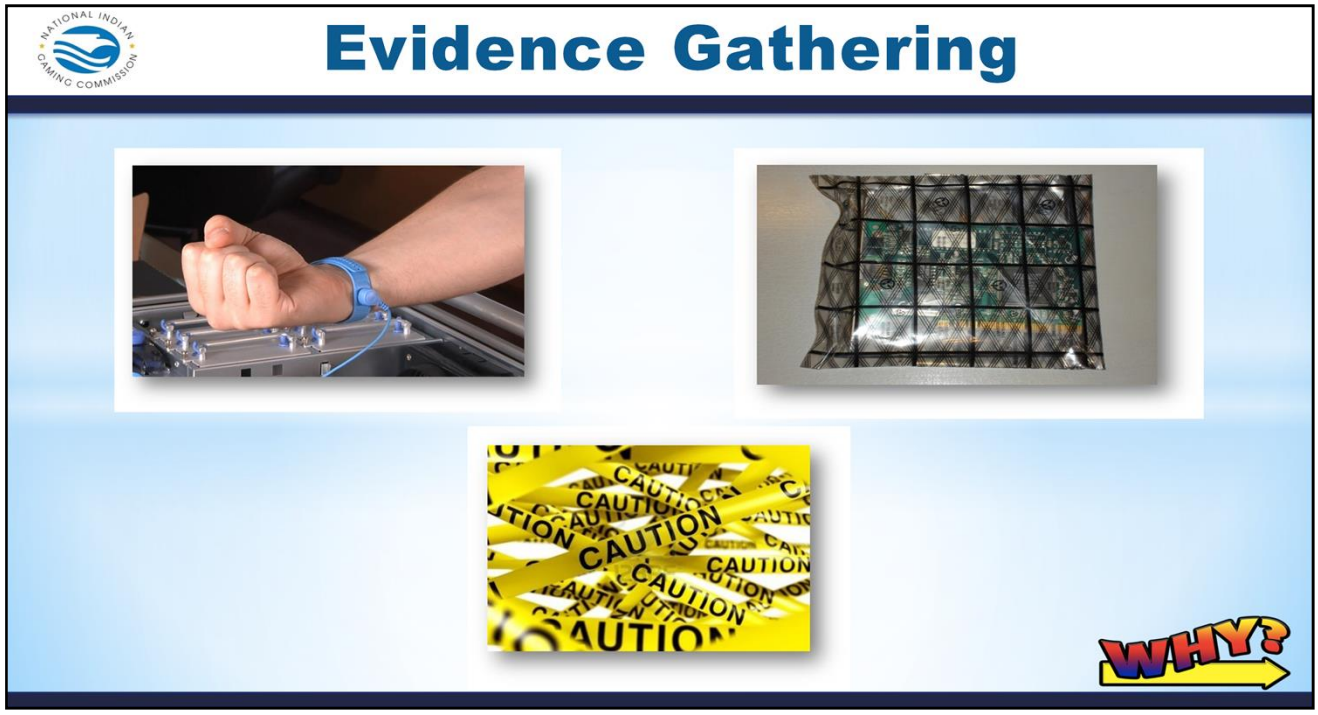
- Miscellaneous handwritten notes (for example, comments written down during previous service)
- Player Promotional Cards
- Tools possibly used to compromise the gaming equipment (screwdrivers, rods, magnets, taser, etc.)
- Hardware and software manuals
- Server/System Generated Reports (Door Entry,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

KEY POINTS

Examples of electronic evidence include:

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

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

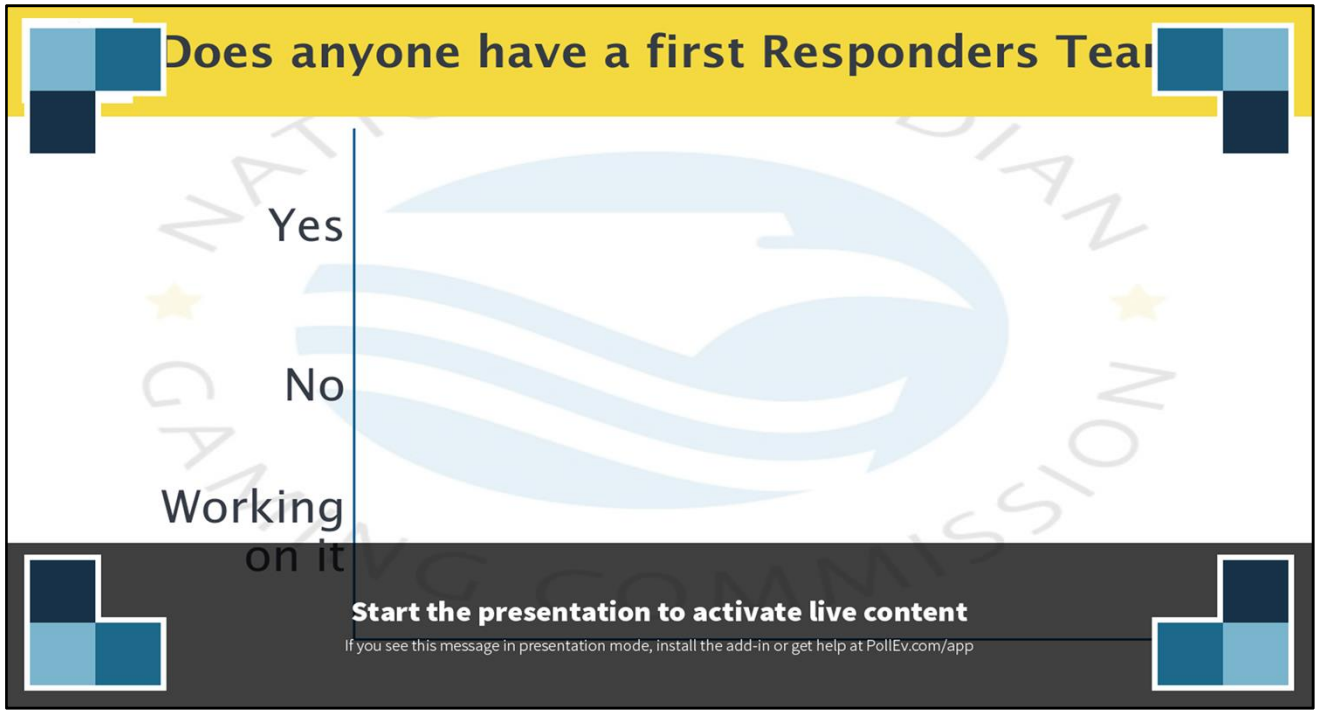


KEY POINTS

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


First Responders
Those directly affecting gaming integrity
❑Regulators
❑Gaming Operations
❑Information Technology
❑Security
❑Surveillance
❑Accounting and Auditing
WHO?

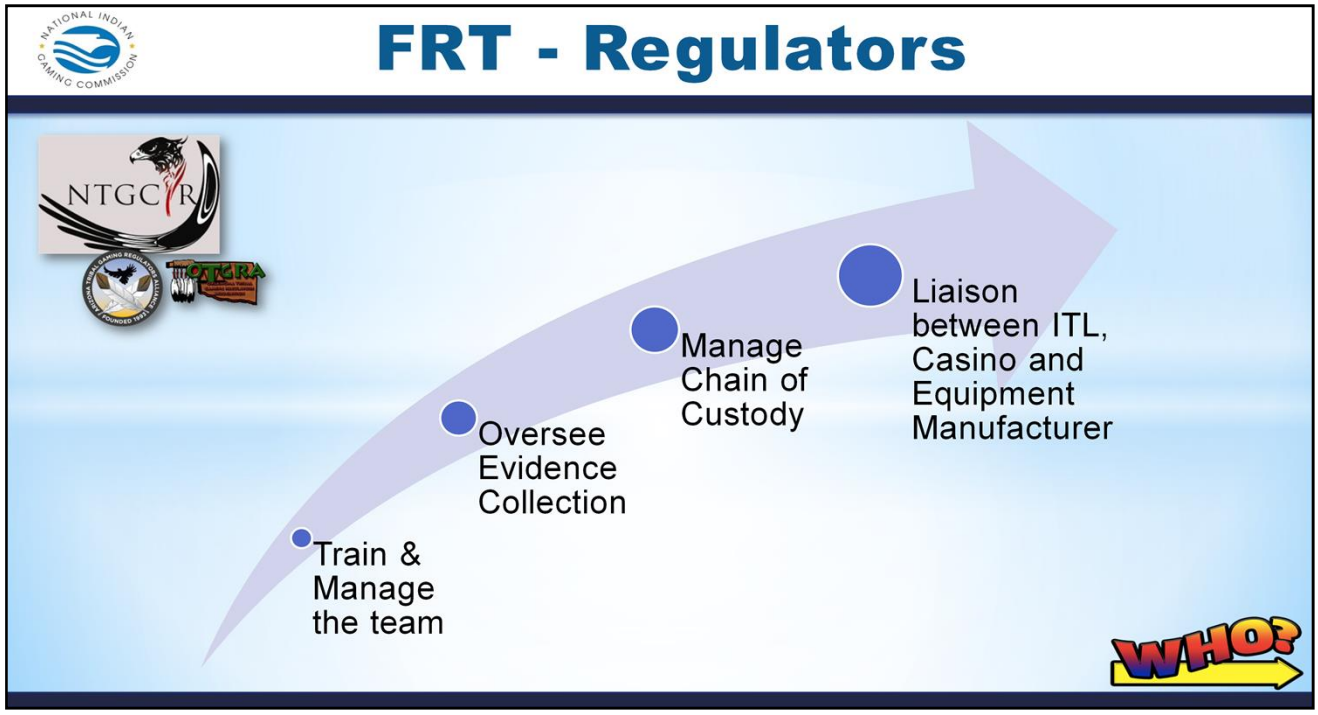
KEY POINTS



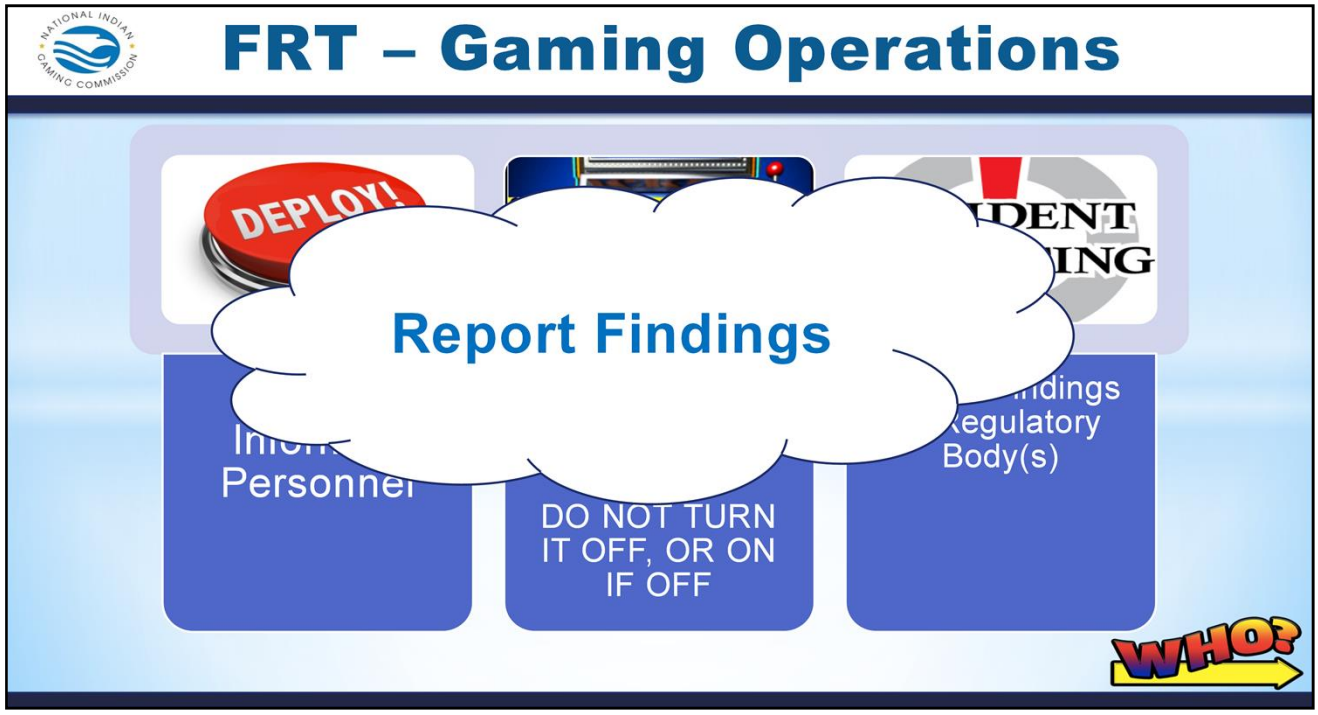
KEY POINTS

Poll Title: Does anyone have a first Responders Team?

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

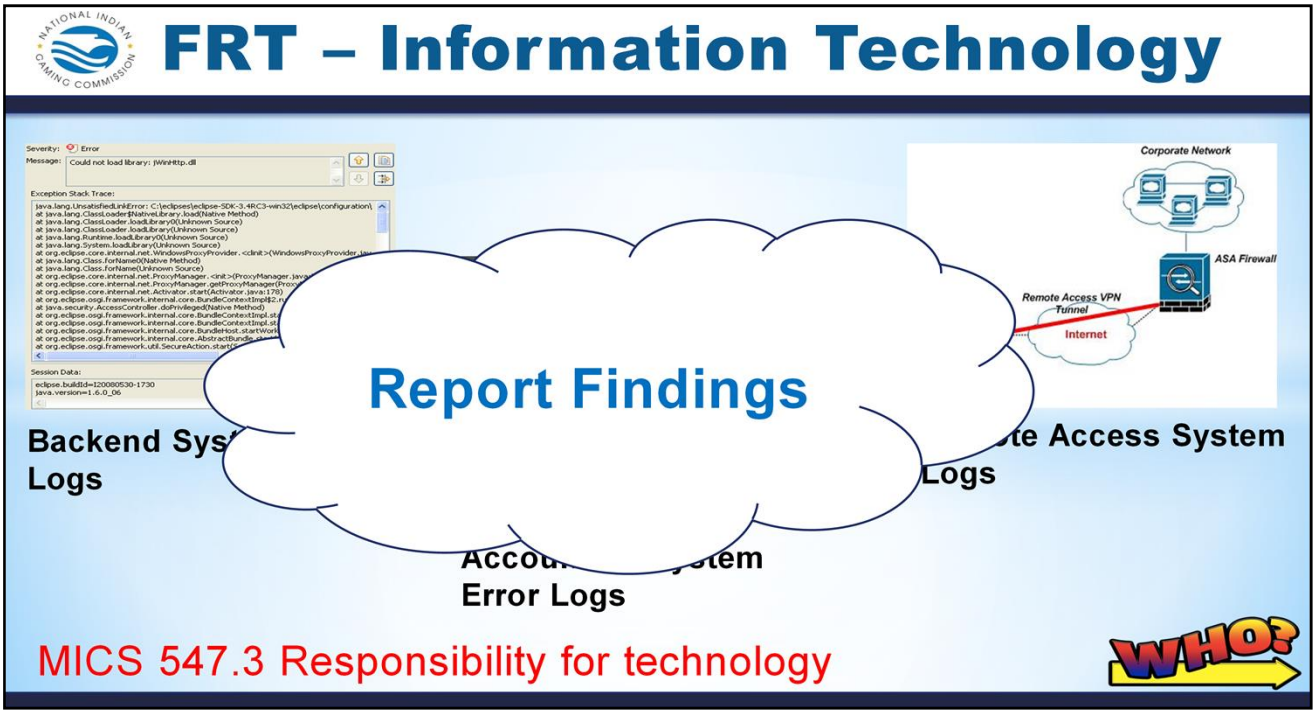

FRT - Regulators
NTGCR
OTGRA
Train & Manage the team
Oversee Evidence Collection
Manage Chain of Custody
Liaison between ITL, Casino and Equipment Manufacturer
WHO?

KEY POINTS



KEY POINTS

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

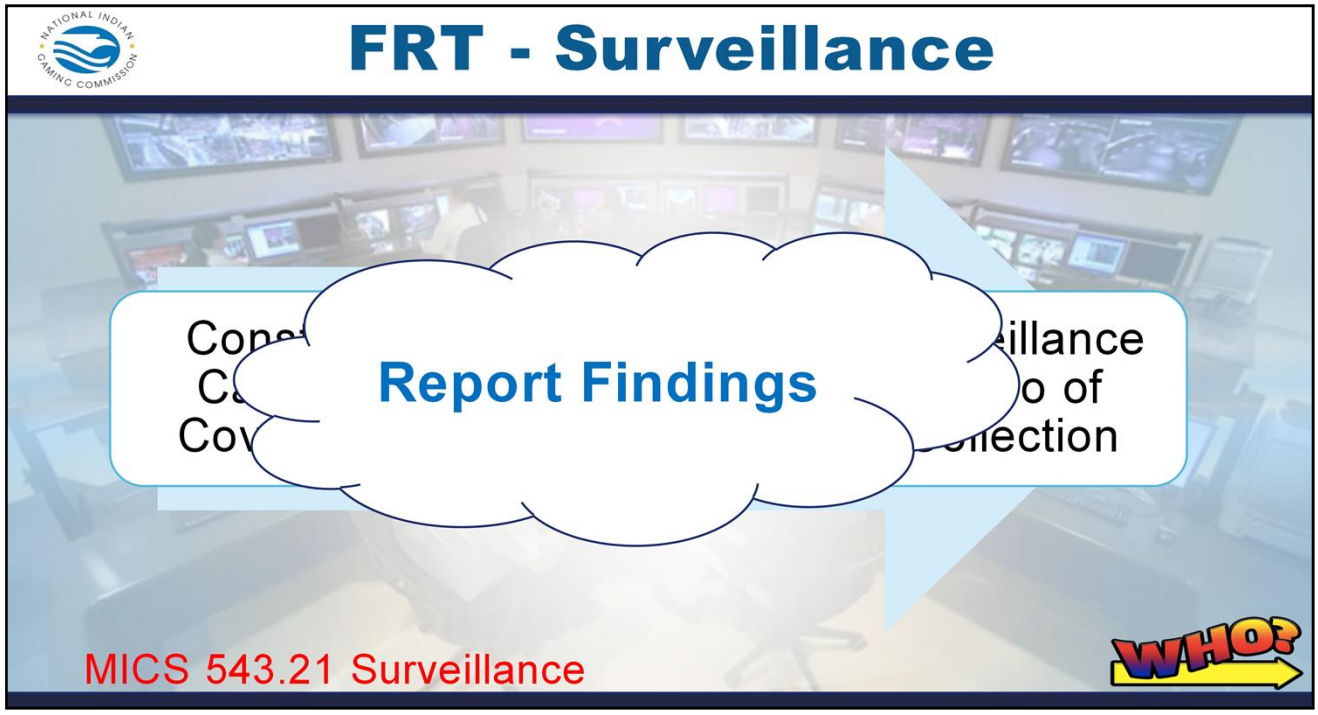


KEY POINTS

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

KEY POINTS

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



KEY POINTS

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

KEY POINTS

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

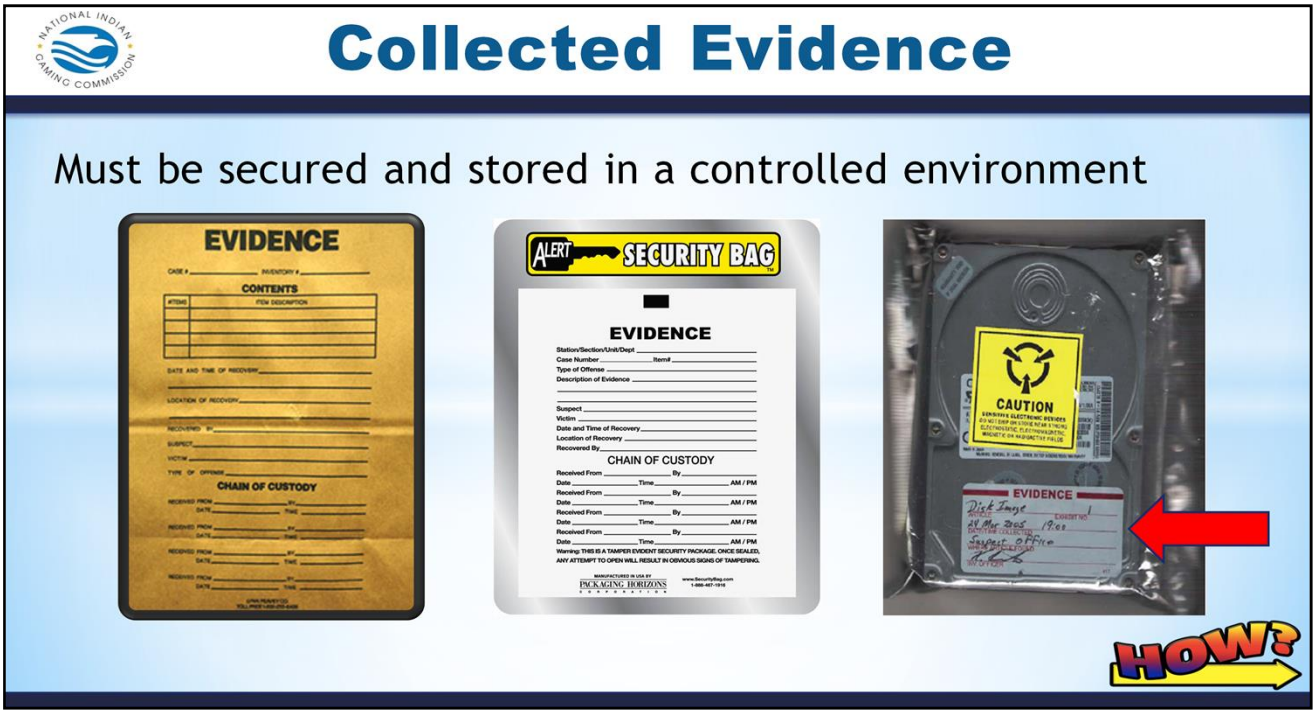

Gaming Commission
As the regulatory body submits information and components for a forensic examination following a thorough investigation and gathering of information and evidence.
IOWA TRIBE
KANSAS - NEBRASKA
ONEIDA
Gaming Commission
POARCH CREEK INDIANS
WHO?

KEY POINTS

KEY POINTS

What should a forensic plan of action consist of?

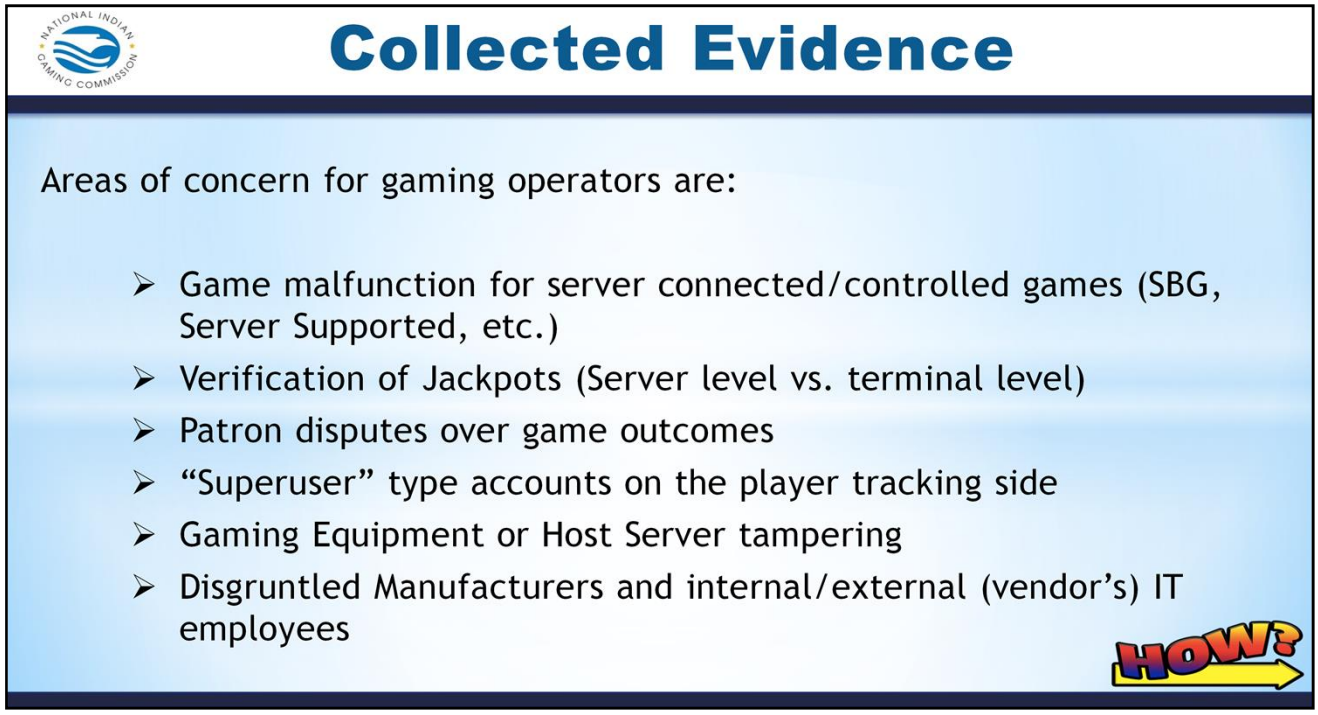
- Establishing a First Responder Team?
- Establishing a Forensic Threshold?
- Escalation guidelines?
- Forensic Readiness Training?



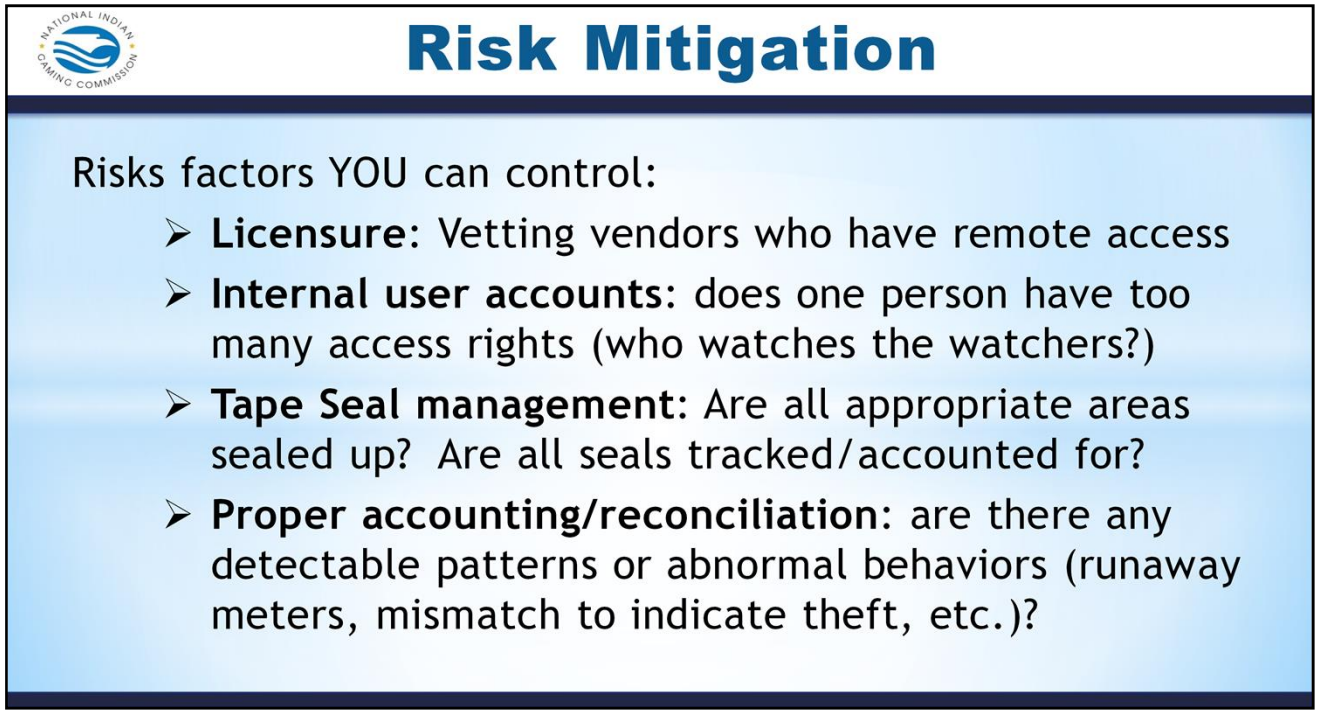
KEY POINTS

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

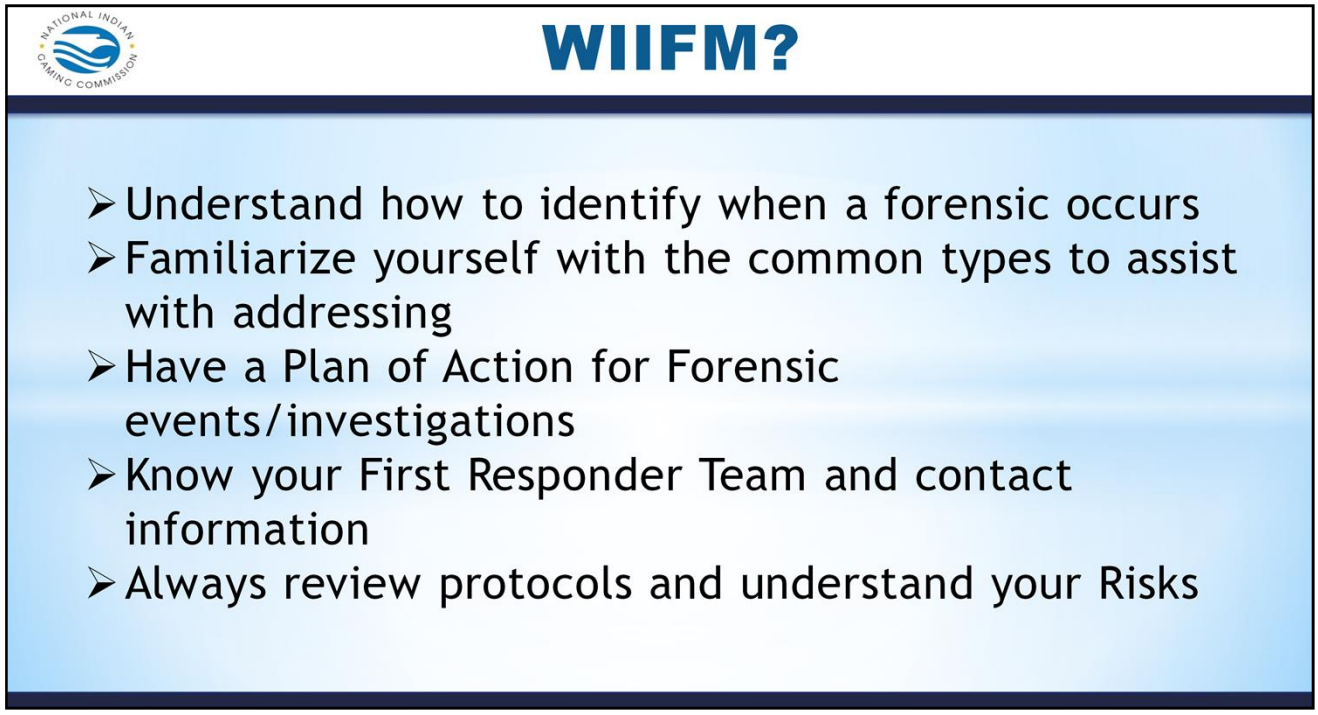
- Proper packaging
- Shipping
- Evidence Repository
- Line of Communication
- Red Arrow reiterate how much date/time signature of individual(s) and proper chain of custody


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

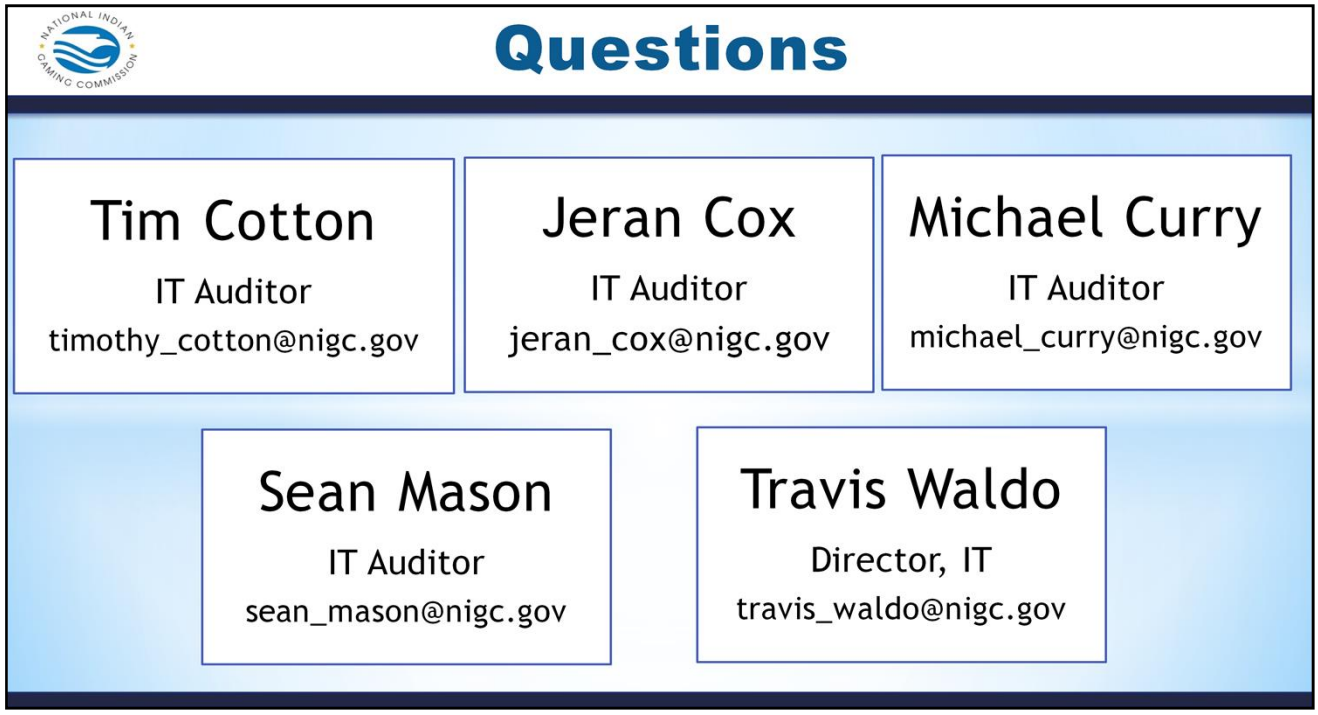
KEY POINTS


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

KEY POINTS


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

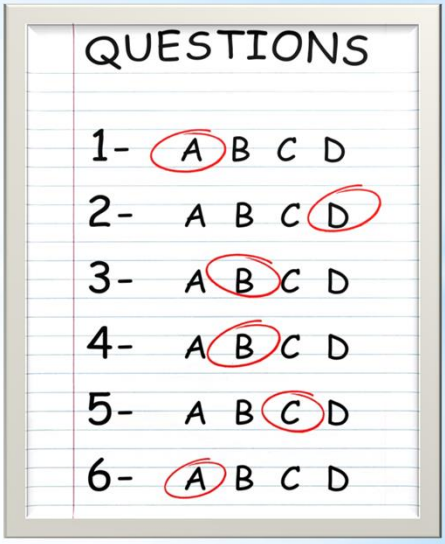
KEY POINTS


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

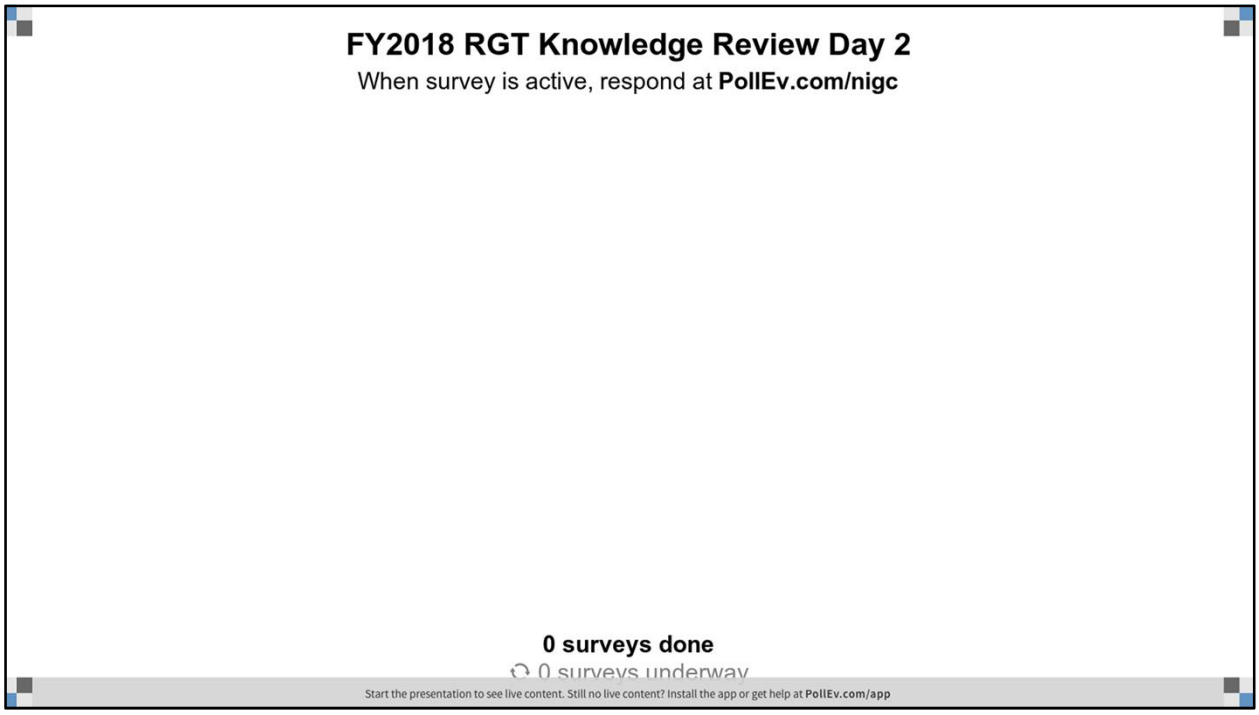
KEY POINTS

Knowledge Review

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



KEY POINTS



Poll Title: FY2018 RGT Knowledge Review Day 2

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

Course Evaluation

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

KEY POINTS

KEY POINTS

Poll Title: Course awe34r567u8i9o0p-[\

IT-107 Forensics in Gaming

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