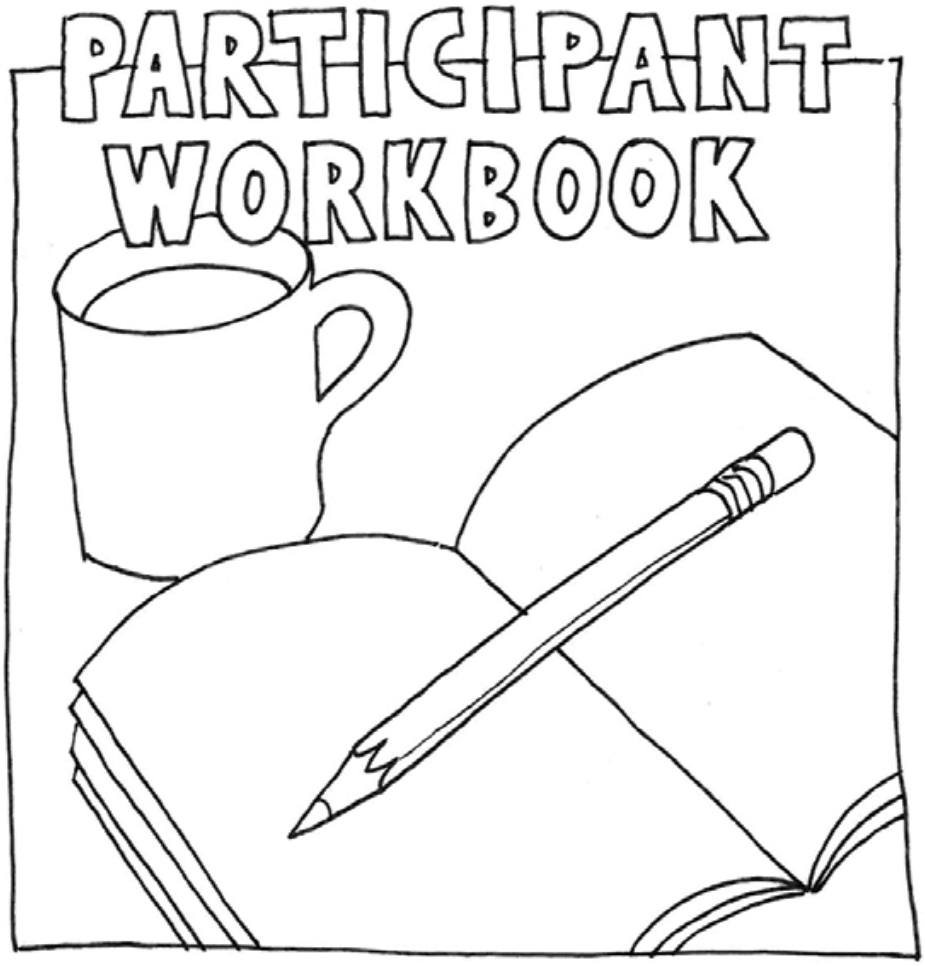
IT Boot Camp



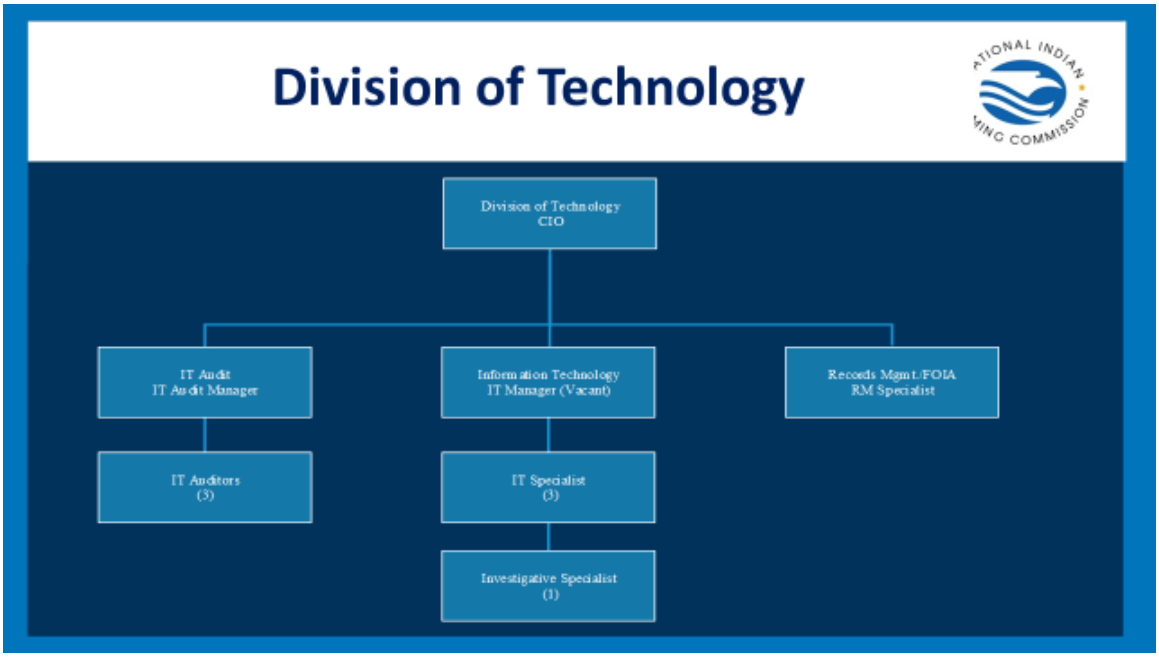
Information Technology Overview

Information Technology

NOTES

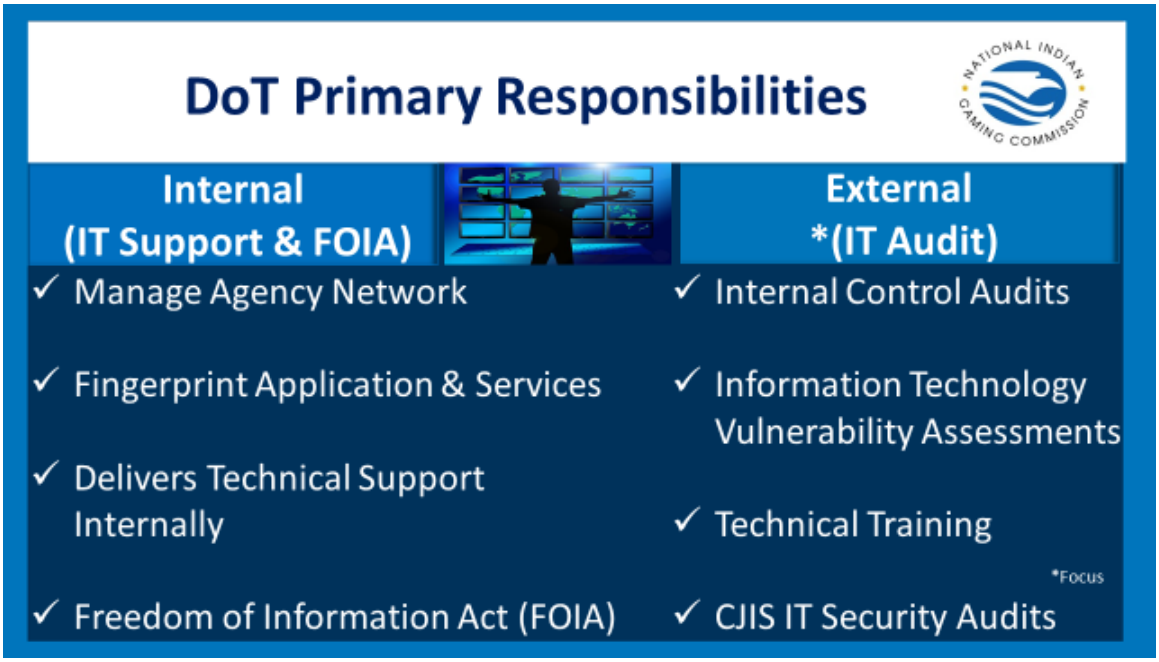

Training Overview
NATIONAL INDIAN GAMING COMMISSION
•Division of Technology (DoT)
•DoT Primary Responsibilities
•IT Audit Responsibilities to Tribal Customers

NOTES



- Chief Information Officer
- Information Technology Audit Team
- Information Technology Team

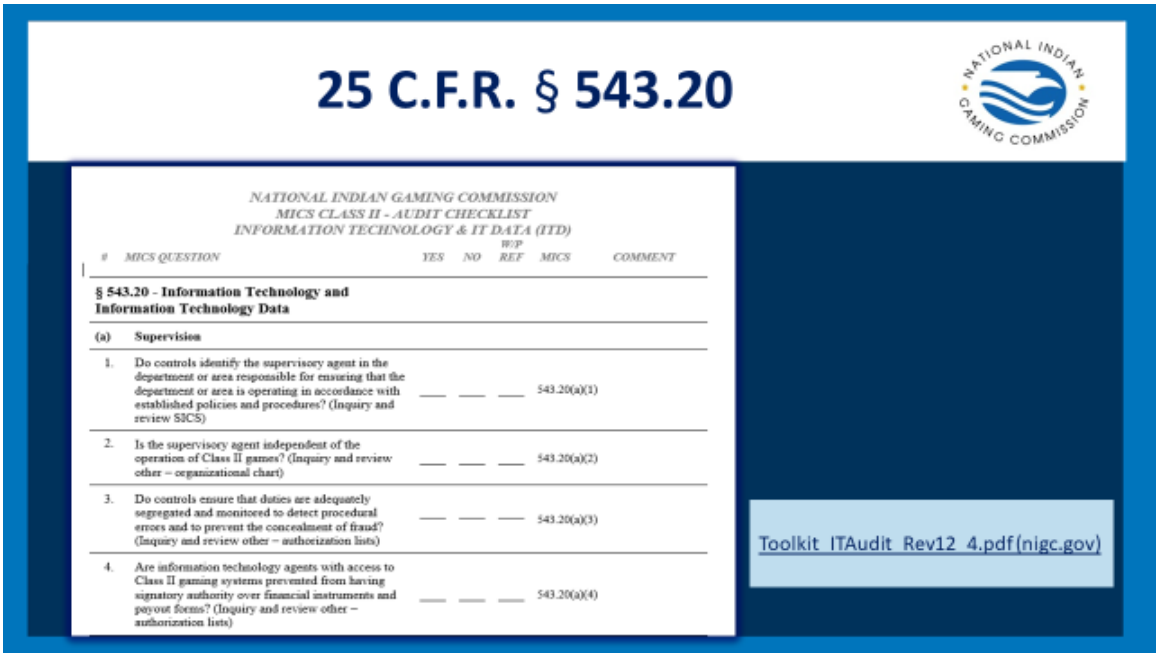
NOTES


DoT Primary Responsibilities
Internal
(IT Support & FOIA)
External
*(IT Audit)
✓ Manage Agency Network
✓ Fingerprint Application & Services
✓ Delivers Technical Support Internally
✓ Freedom of Information Act (FOIA)
✓ Internal Control Audits
✓ Information Technology Vulnerability Assessments
✓ Technical Training
*Focus
✓ CJIS IT Security Audits

NOTES

Effective since 2013 for Class II Gaming

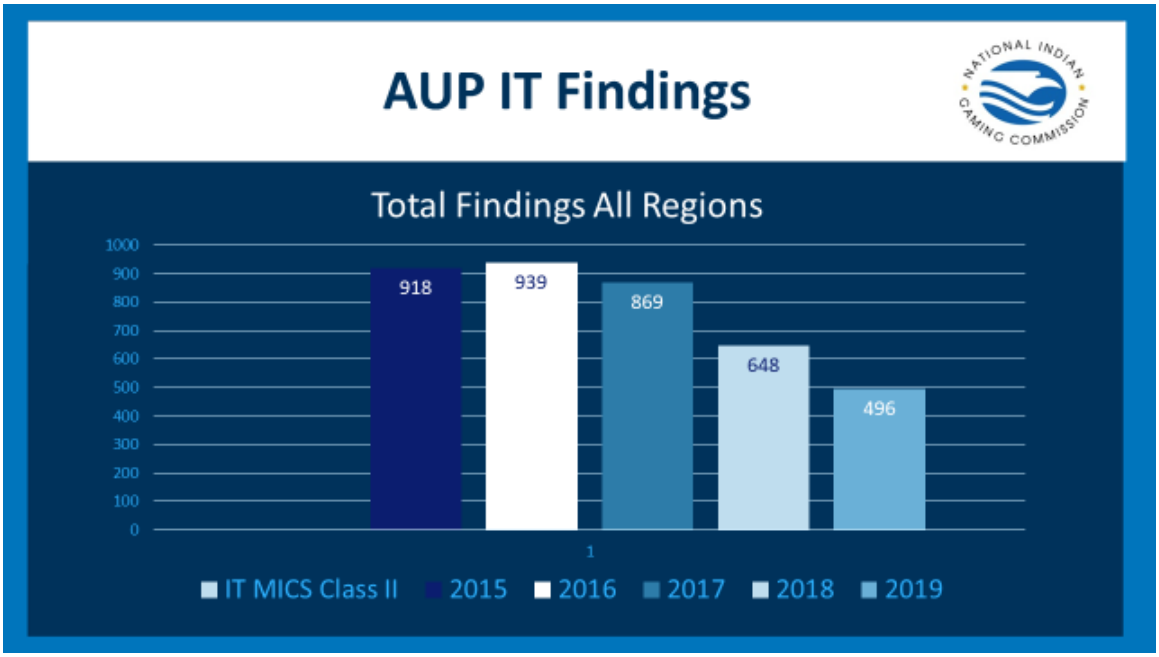
NOTES



The IT portion of an internal audit conducted by the NIGC…reference the 543.20 toolkit "Click the LINK for Toolkit" after reading the information below.
https://www.nigc.gov/images/uploads/training/Toolkit_ITAudit_Rev12_4.pdf

NOTES

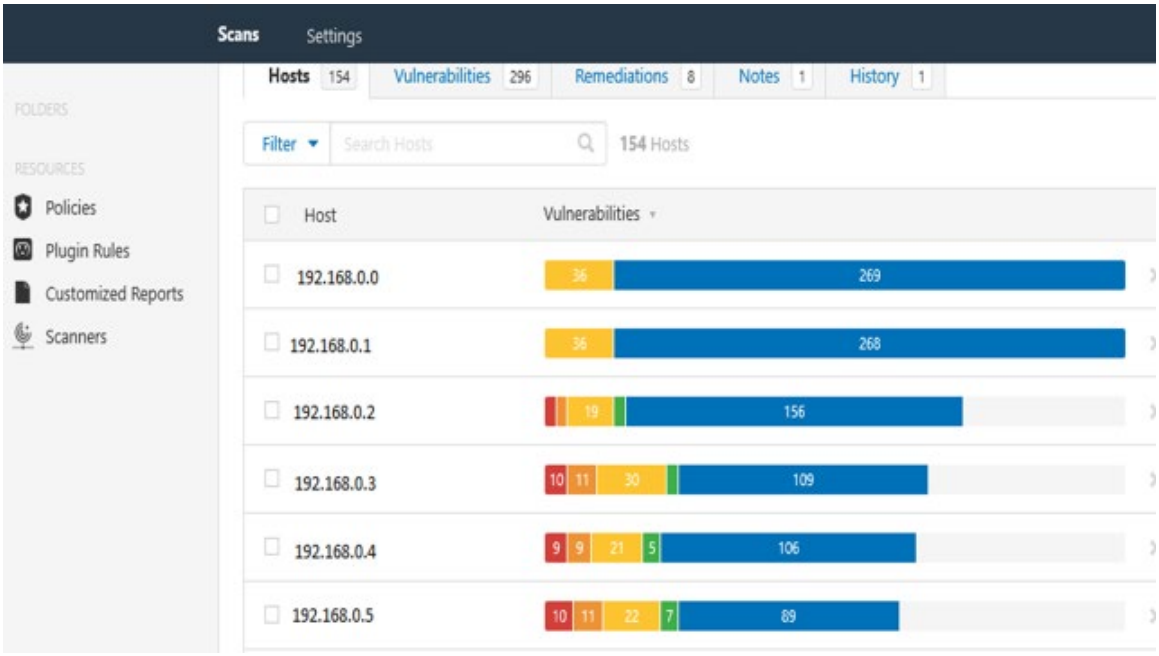
With the uptick of Cyber attacks especially in Indian Country, we need to ensure that the Operational IT side of the house has proper P&Ps in place.



Top 5 findings/standards for 2019: _____of the top 5 findings centers around User Controls

- 543.20(f)(5) – User Controls - Access credentials of terminated users must be deactivated within an established time period approved by the TGRA. - _____
- 543.20(i)(2) – Incident Monitoring - All security incidents must be responded to within an established time period approved by the TGRA and formally documented. - _____
- 543.20(f)(3)(ii) – Access Credentials must be changed at an established interval approved by the TGRA;- _____
- 543.20(f)(4) – User Controls - Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.- _____
- 543.20(e)(1)(i) – Logical Security - Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:
    - Systems' software and application programs - _____

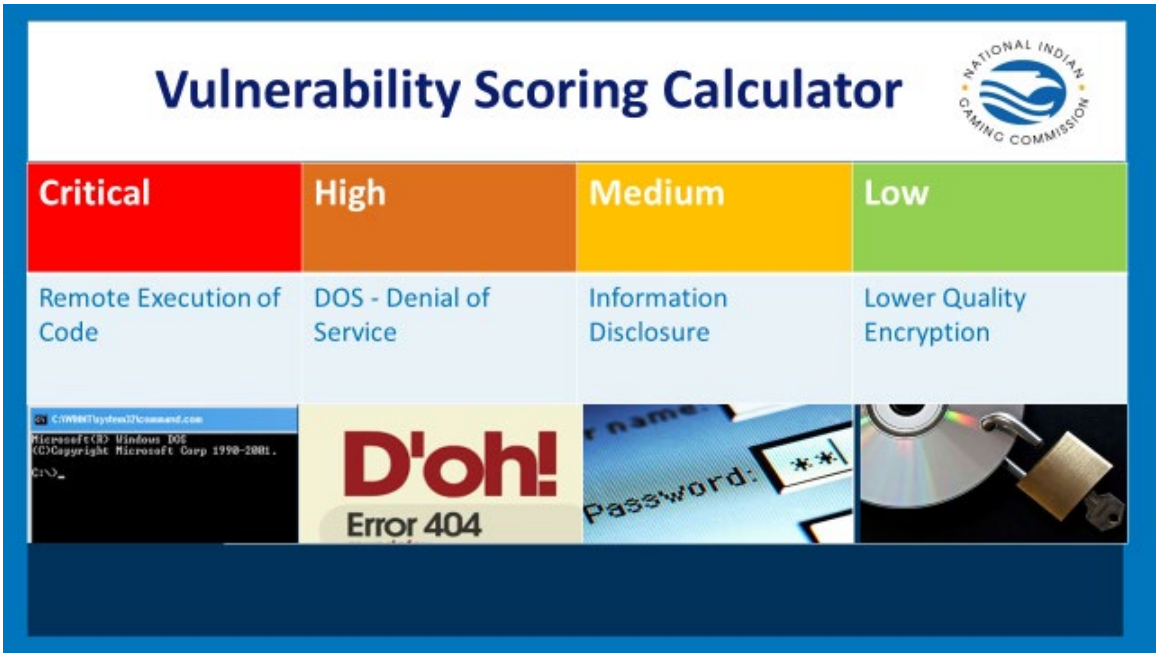
Information Technology Vulnerability Assessment



Sample scan during an ITVA

A vulnerability assessment is the **process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems**, applications and network infrastructures and **providing the organization** doing the assessment **with the necessary knowledge, awareness and risk** background **to understand the threats** to its environment and react appropriately.

NOTE:



NIGC uses industry standard software to automate much of the process of finding vulnerabilities.

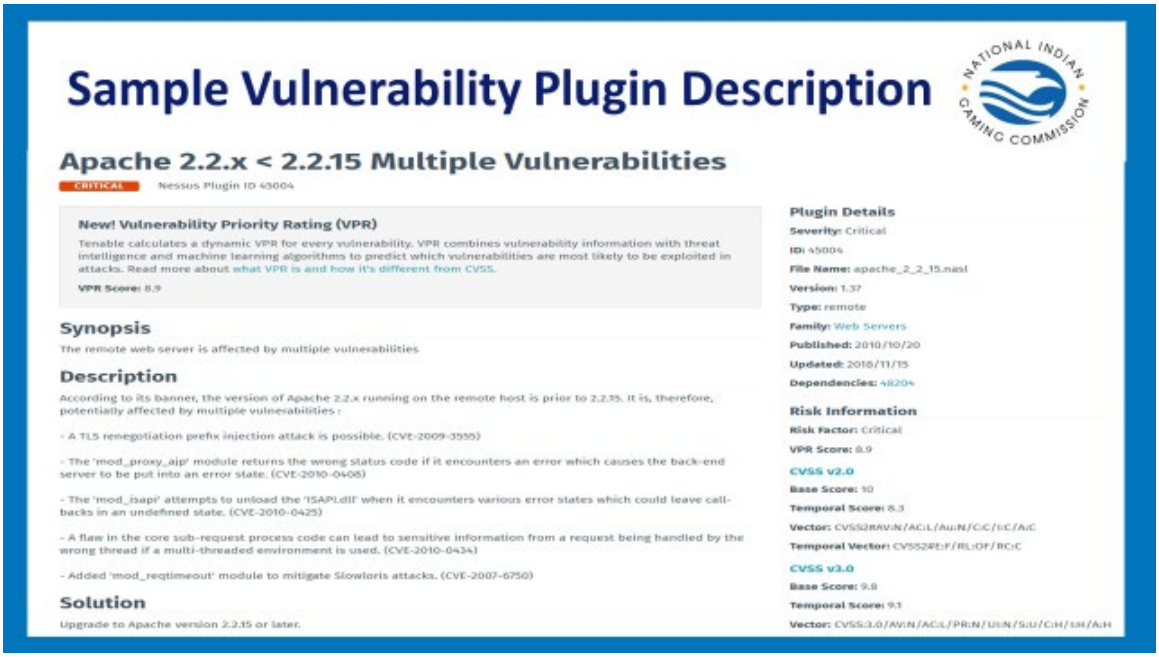
Tenable Nessus and **Metasploit** are two of the most well known utilities.

The respective software bases the severity of the vulnerabilities off published databases from:

- NIST (National Institute of Standards and Technology)
- CVSS (Common Vulnerability Scoring System)
- NVD (National Vulnerability Database)

  See also:
  https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=AV:N/AC:L/Au:N/C:P/I:P/A:P

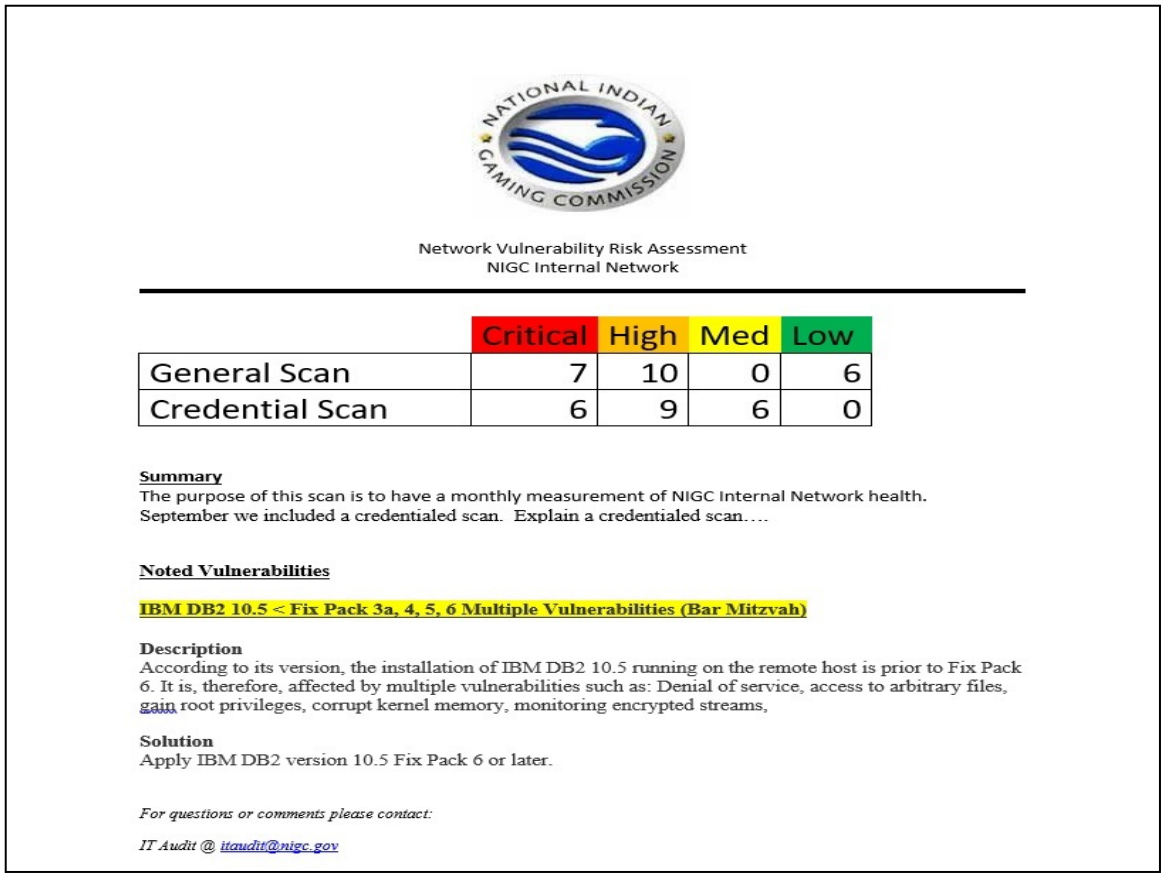
NOTES



Why this information is important?

1. **Older Network Infrastructures** – allow for _____into player tracking data or cyber attacks
2. **Windows XP/7/Old PC's** – End of Life PCs with no _____ allowing for security concerns and accessibility by unwanted online attackers
3. **Missing Software Patches** – Updated software patches assist with keeping software up to date to not allow _____ identified by the software vendor
4. **Open Network Ports** – Unmanaged ports or just open ports with _____allow for persons to possibly jump onto a network and cause harm.

NIGC Sample Vulnerability Report



Network Vulnerability Risk Assessment
NIGC Internal Network

	Critical	High	Med	Low
General Scan	7	10	0	6
Credential Scan	6	9	6	0

Summary
The purpose of this scan is to have a monthly measurement of NIGC Internal Network health. September we included a credentialed scan. Explain a credentialed scan….

Noted Vulnerabilities

IBM DB2 10.5 < Fix Pack 3a, 4, 5, 6 Multiple Vulnerabilities (Bar Mitzvah)

Description
According to its version, the installation of IBM DB2 10.5 running on the remote host is prior to Fix Pack 6. It is, therefore, affected by multiple vulnerabilities such as: Denial of service, access to arbitrary files, gain root privileges, corrupt kernel memory, monitoring encrypted streams,

Solution
Apply IBM DB2 version 10.5 Fix Pack 6 or later.

For questions or comments please contact:

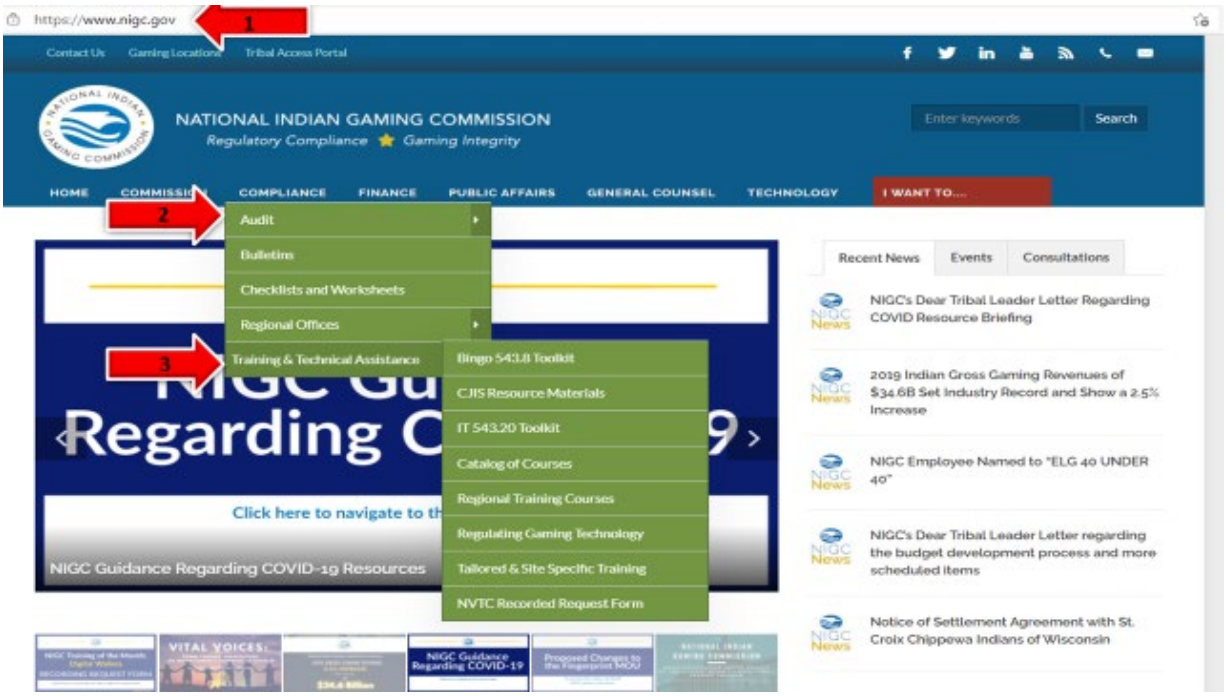
IT Audit @ itaudit@nigc.gov

NOTES

Technical Training

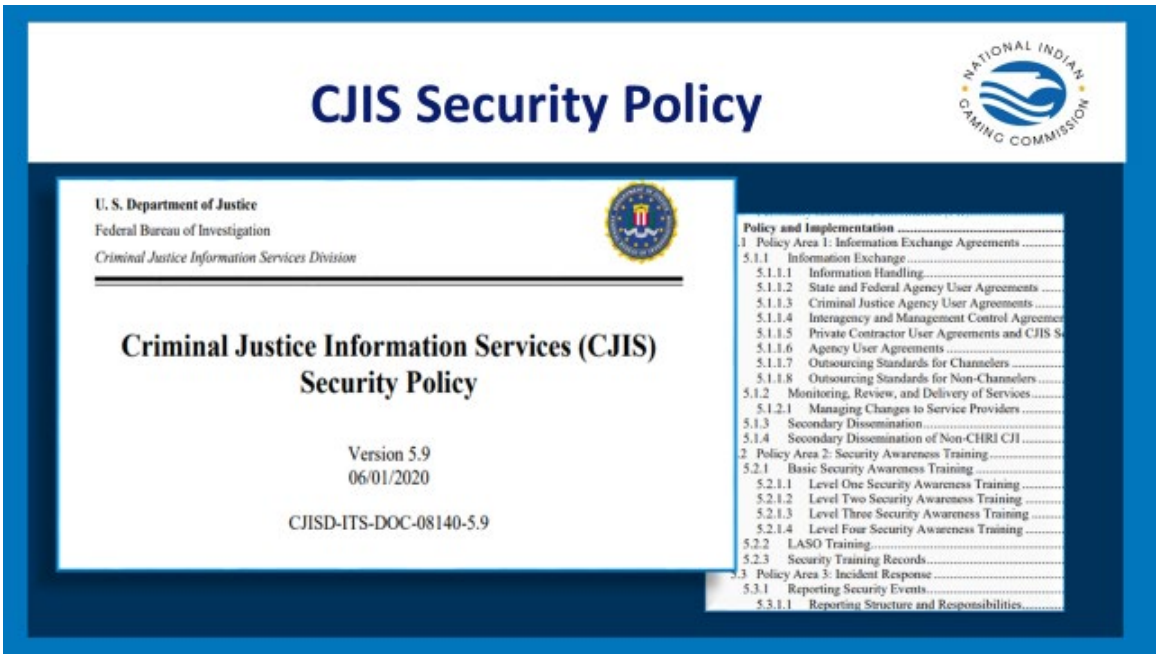
You can request trainings at www.nigc.gov. All training inquiries can be sent to traininginfo@nigc.gov.

NOTES


https://www.nigc.gov
1
Contact Us
Gaming Locations
Tribal Access Portal
NATIONAL INDIAN GAMING COMMISSION
Regulatory Compliance ★ Gaming Integrity
Enter keywords
Search
HOME
COMMISSION
COMPLIANCE
FINANCE
PUBLIC AFFAIRS
GENERAL COUNSEL
TECHNOLOGY
I WANT TO...
2
Audit
Bulletins
Checklists and Worksheets
Regional Offices
3
Training & Technical Assistance
Bingo 543.8 Toolkit
CJIS Resource Materials
IT 543.20 Toolkit
Catalog of Courses
Regional Training Courses
Regulating Gaming Technology
Tailored & Site Specific Training
NVTC Recorded Request Form
Click here to navigate to th
NIGC Guidance Regarding COVID-19 Resources
Recent News
Events
Consultations
NIGC's Dear Tribal Leader Letter Regarding COVID Resource Briefing
2019 Indian Gross Gaming Revenues of $34.6B Set Industry Record and Show a 2.5% Increase
NIGC Employee Named to "ELG 40 UNDER 40"
NIGC's Dear Tribal Leader Letter regarding the budget development process and more scheduled items
Notice of Settlement Agreement with St. Croix Chippewa Indians of Wisconsin

NOTES

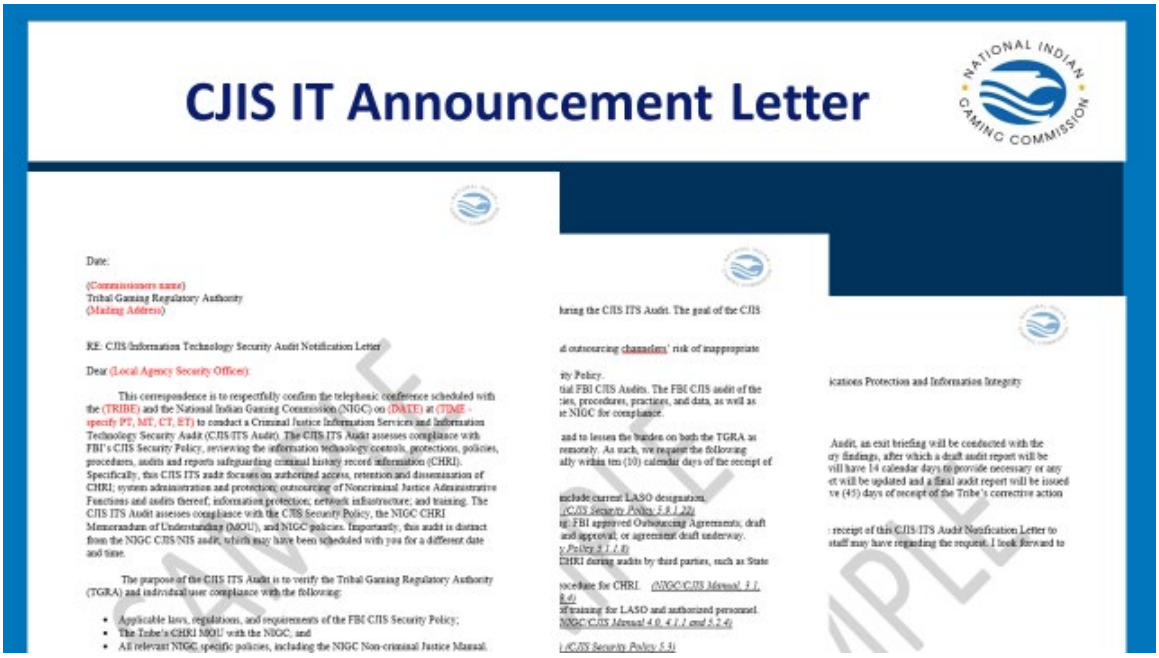
CJIS Information Technology Audits



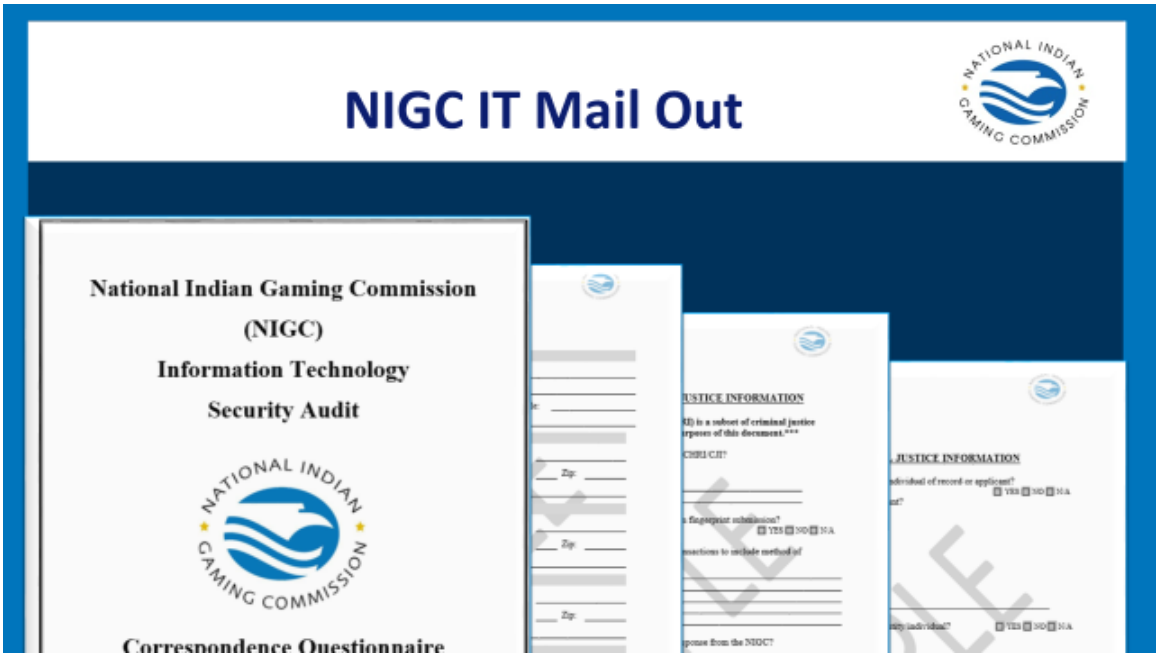
Criminal Justice Information Services (CJIS) Security Policy — FBI

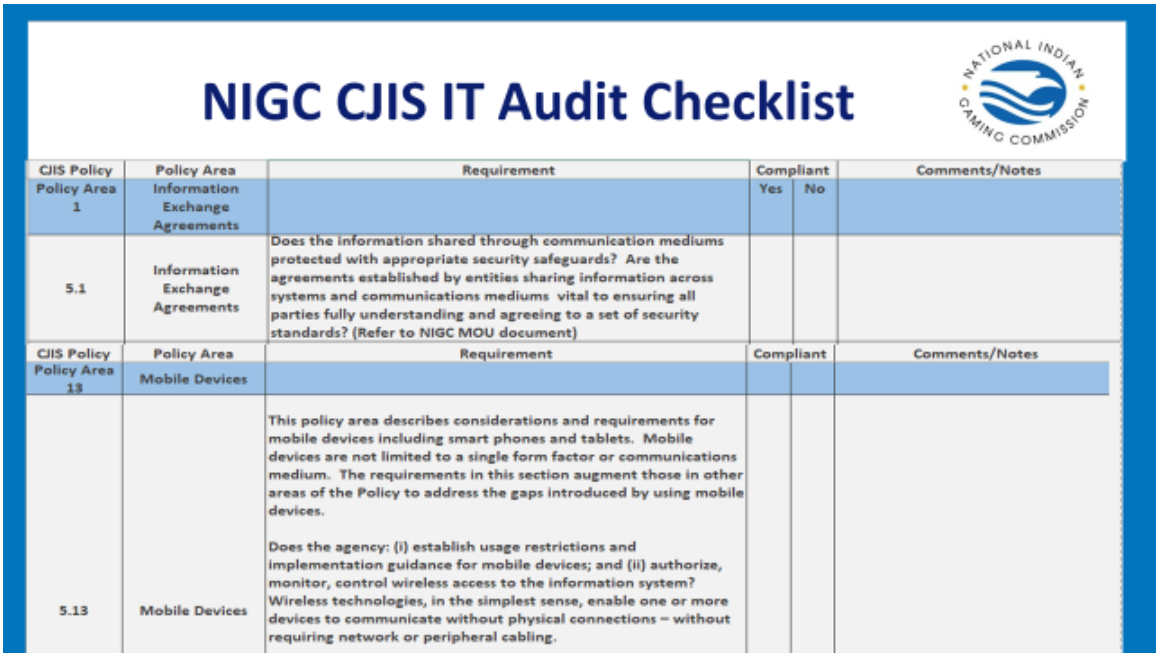
https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

NOTES


CJIS IT Announcement Letter
NATIONAL INDIAN GAMING COMMISSION
Date:
(Commissioners name)
Tribal Gaming Regulatory Authority
(Mailing Address)
RE: CJIS/Information Technology Security Audit Notification Letter
Dear (Local Agency Security Officer):
This correspondence is to respectfully confirm the telephonic conference scheduled with the (TRIBE) and the National Indian Gaming Commission (NIGC) on (DATE) at (TIME - specify PT, MT, CT, ET) to conduct a Criminal Justice Information Services and Information Technology Security Audit (CJIS/ITS Audit). The CJIS ITS Audit assesses compliance with FBI's CJIS Security Policy, reviewing the information technology controls, protections, policies, procedures, audits and reports safeguarding criminal history record information (CHRI). Specifically, this CJIS ITS audit focuses on authorized access, retention and dissemination of CHRI; system administration and protection; outsourcing of Noncriminal Justice Administrative Functions and audits thereof; information protection; network infrastructure; and training. The CJIS ITS Audit assesses compliance with the CJIS Security Policy, the NIGC CHRI Memorandum of Understanding (MOU), and NIGC policies. Importantly, this audit is distinct from the NIGC CJIS/NIS audit, which may have been scheduled with you for a different date and time.
The purpose of the CJIS ITS Audit is to verify the Tribal Gaming Regulatory Authority (TGRA) and individual user compliance with the following:
Applicable laws, regulations, and requirements of the FBI CJIS Security Policy;
The Tribe's CHRI MOU with the NIGC; and
All relevant NIGC specific policies, including the NIGC Non-criminal Justice Manual.
during the CJIS ITS Audit. The goal of the CJIS
d outsourcing channelers' risk of inappropriate
ity Policy.
tial FBI CJIS Audits. The FBI CJIS audit of the
cies, procedures, practices, and data, as well as
e NIGC for compliance.
and to lessen the burden on both the TGRA as
remotely. As such, we request the following
ally within ten (10) calendar days of the receipt of
include current LASO designation.
(CJIS Security Policy 5.8.1.2(2))
g: FBI approved Outsourcing Agreements; draft
and approval; or agreement draft underway.
y Policy 5.1.1.8)
CHRI during audits by third parties, such as State
ocedure for CHRI. (NIGC/CJIS Manual 3.1,
ll.4)
of training for LASO and authorized personnel.
NIGC CJIS Manual 4.0, 4.1.1 and 5.2.4)
(CJIS Security Policy 5.3)
ications Protection and Information Integrity
Audit, an exit briefing will be conducted with the
ary findings, after which a draft audit report will be
will have 14 calendar days to provide necessary or any
et will be updated and a final audit report will be issued
ve (45) days of receipt of the Tribe's corrective action
receipt of this CJIS/ITS Audit Notification Letter to
staff may have regarding the request. I look forward to

NOTES


NIGC IT Mail Out
NATIONAL INDIAN GAMING COMMISSION
National Indian Gaming Commission
(NIGC)
Information Technology
Security Audit
NATIONAL INDIAN GAMING COMMISSION
Correspondence Questionnaire



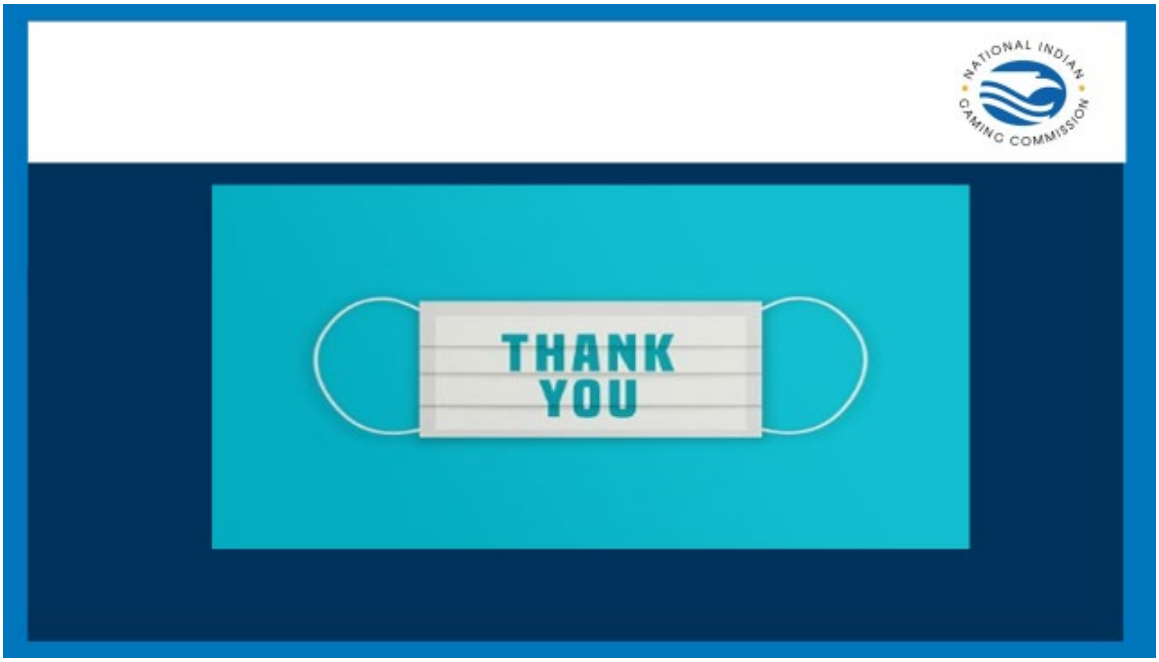
NIGC CJIS IT Audit Checklist

CJIS Policy	Policy Area	Requirement	Compliant		Comments/Notes
Policy Area 1	Information Exchange Agreements		Yes	No	
5.1	Information Exchange Agreements	Does the information shared through communication mediums protected with appropriate security safeguards? Are the agreements established by entities sharing information across systems and communications mediums vital to ensuring all parties fully understanding and agreeing to a set of security standards? (Refer to NIGC MOU document)			
CJIS Policy	Policy Area	Requirement	Compliant		Comments/Notes
Policy Area 13	Mobile Devices				
5.13	Mobile Devices	This policy area describes considerations and requirements for mobile devices including smart phones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices. Does the agency: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system? Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections – without requiring network or peripheral cabling.			

NOTES


IT Audit Recap
NATIONAL INDIAN GAMING COMMISSION
✓ Internal Control Audits (ICA)
✓ Information Technology Vulnerability Assessments (ITVA)
✓ Technical Training and Assistance
✓ CJIS IT Security Audits

NOTES



Thank you for your participation and attending this session of the Information Technology Boot Camp!

After you log out you will receive a Survey. We ask that you complete the survey as the feedback helps us to get better at what we do!

We hope that you will join us for the next session.

NIGC Training can be reached at traininginfo@nigc.gov