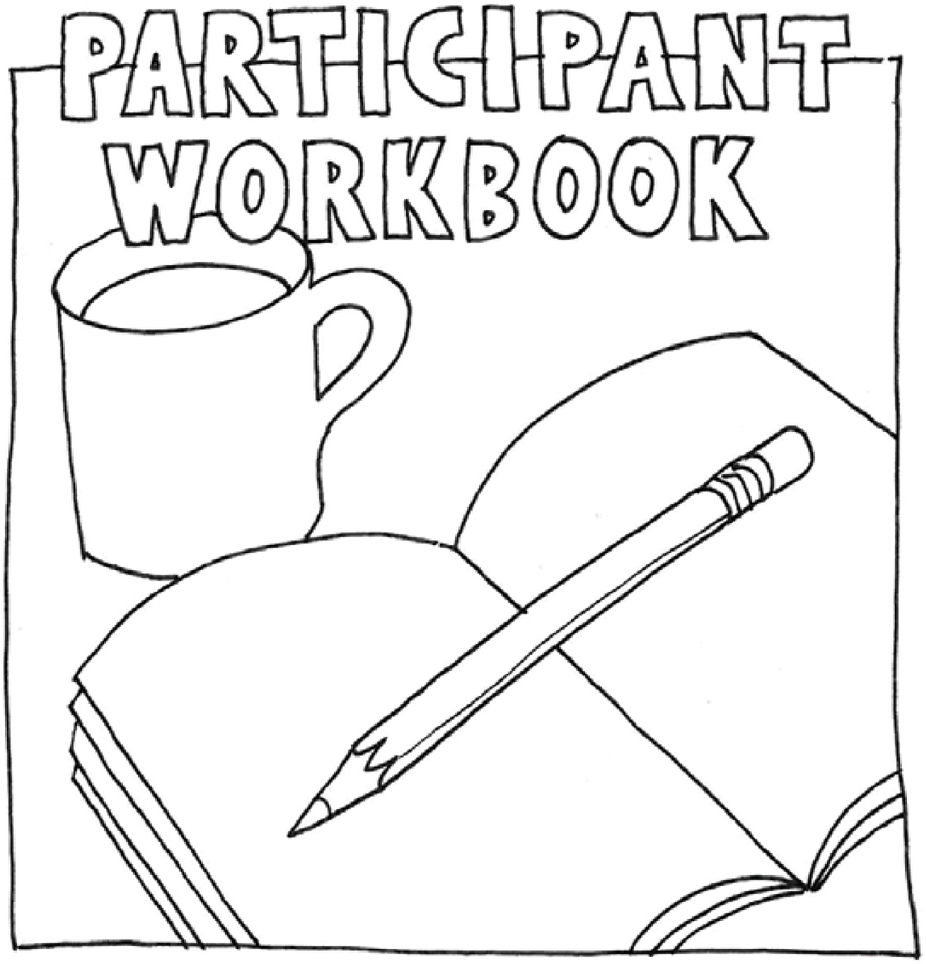
IT Boot Camp



CJIS IT Security Audit Overview –Part II

Part II:

NIGC CJIS IT Security Audits – Part II

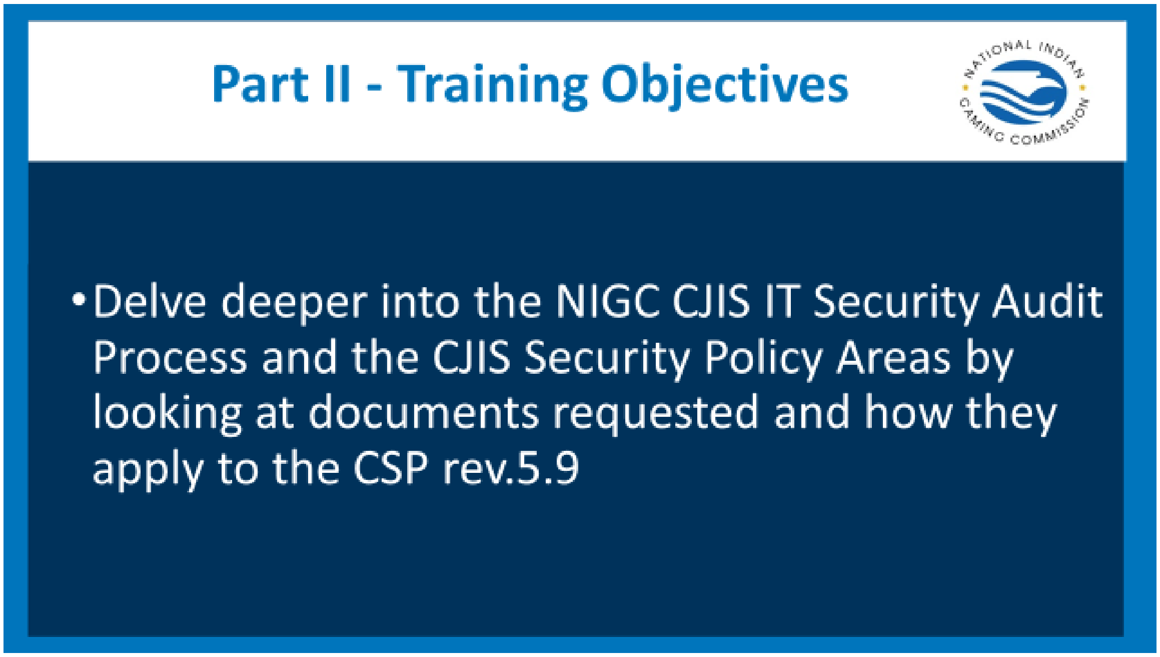
CJIS Security Policy v5.9 & CJIS IT Security Audits

Division of Technology

NATIONAL INDIAN GAMING COMMISSION

Welcome back. This is the continuation of the Fingerprint process and CJIS Security Policy course. In this section, we will dive deeper into the individual CJIS policy areas as well as, expand upon the NIGC CJIS IT Security Audit process.

NOTES

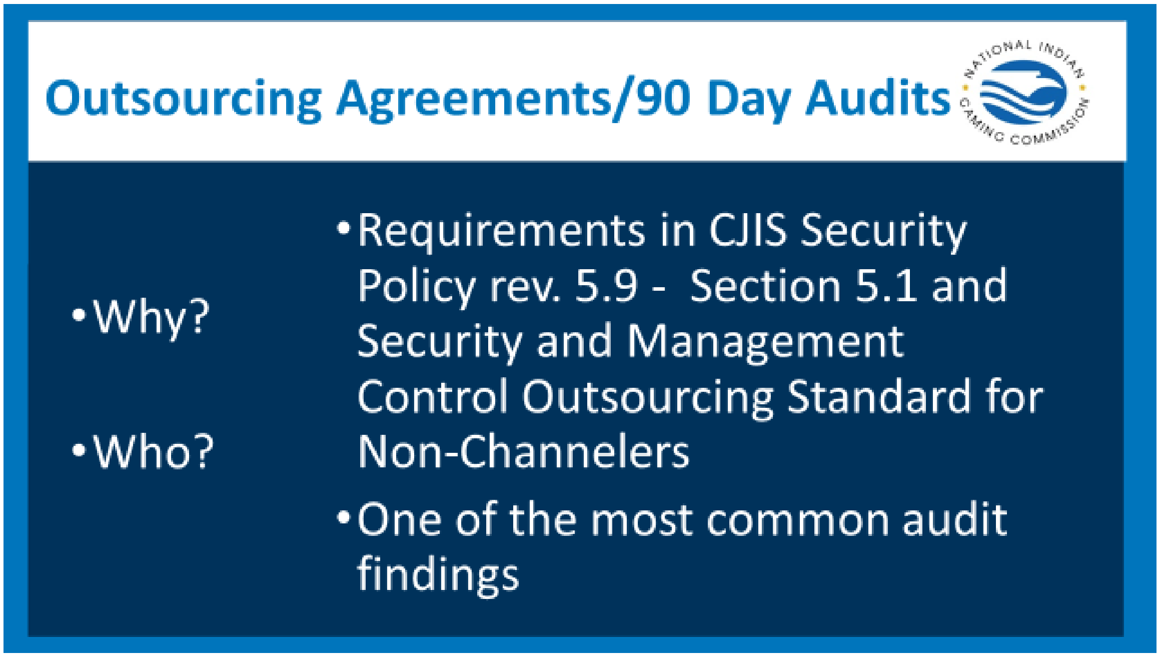


Part II - Training Objectives

- Delve deeper into the NIGC CJIS IT Security Audit Process and the CJIS Security Policy Areas by looking at documents requested and how they apply to the CSP rev.5.9

These examples are not meant to be exhaustive and do not cover every policy area in the CSP, just some of the ones related to commonly requested documents of a NIGC CJIS IT Sec Audit

NOTES



Outsourcing Agreements/90 Day Audits

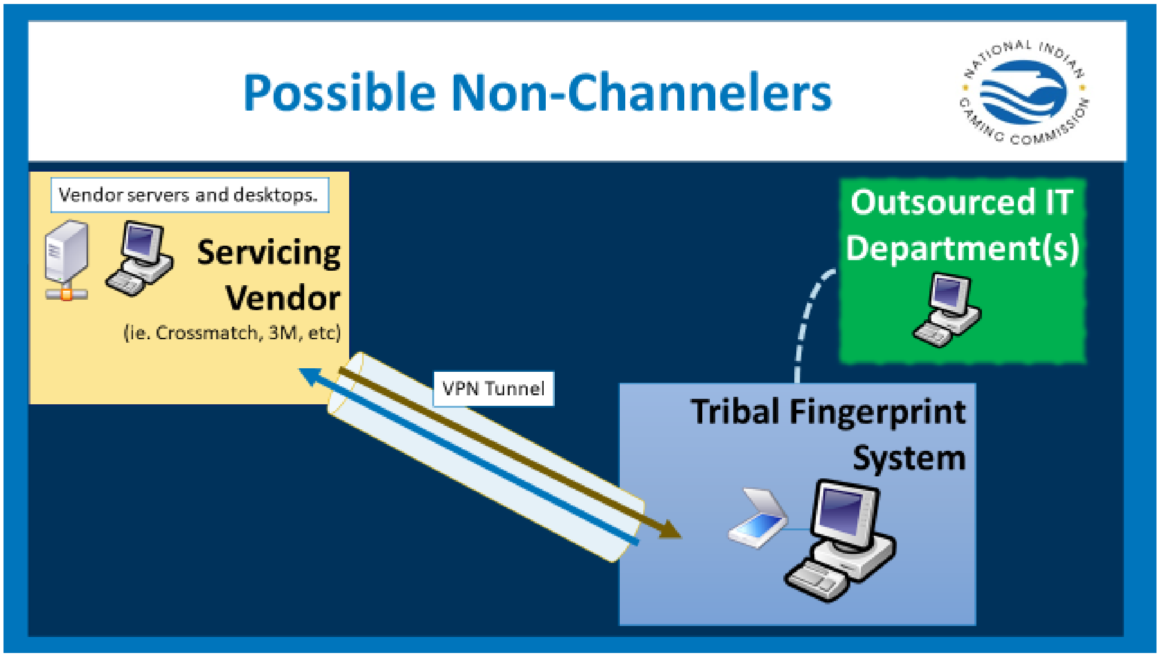
- Why?
- Who?

- Requirements in CJIS Security Policy rev. 5.9 - Section 5.1 and Security and Management Control Outsourcing Standard for Non-Channelers
- One of the most common audit findings

Why is this needed?

> Due to the requirements in CSP 5.1, sometimes called the “compact council” or OS document. This document details the requirements regarding Non-Channelers.

NOTES



Possible Non-Channelers

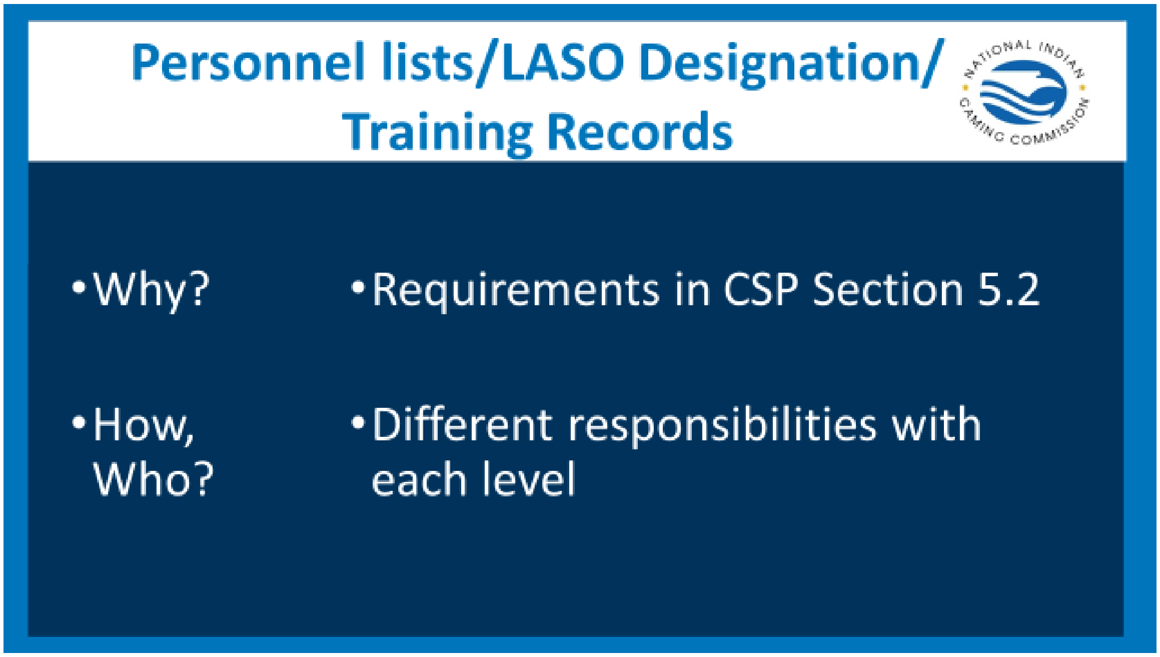
Vendor servers and desktops.
Servicing Vendor
(ie. Crossmatch, 3M, etc)
VPN Tunnel
Outsourced IT Department(s)
Tribal Fingerprint System

Let’s return to the earlier network diagram slide in Part 1, but this time let’s declutter it and focus just on the most common or likely “non-channelers”

Some of the more common scenarios.

- Outsourced IT departments helping to maintain tribal fingerprint systems and related networks
- The manufacturers and vendors of the fingerprint system scanners and software

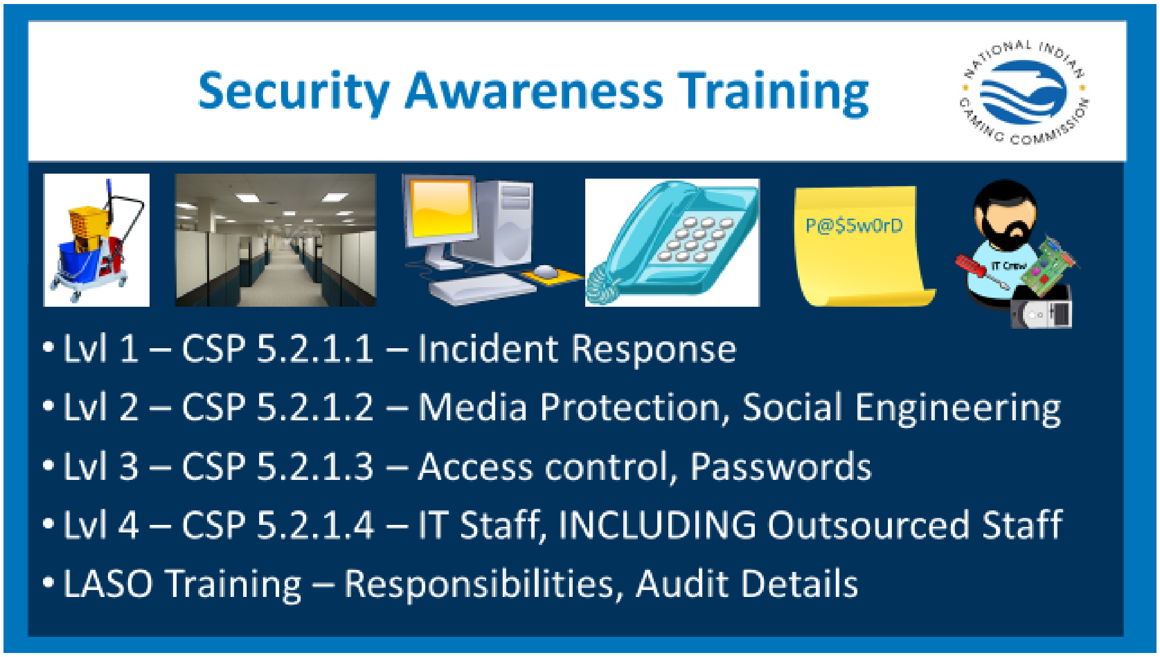
NOTES



Personnel lists/LASO Designation/ Training Records

• Why?	• Requirements in CSP Section 5.2
• How, Who?	• Different responsibilities with each level

NOTES


P@$5w0rD
IT Crew

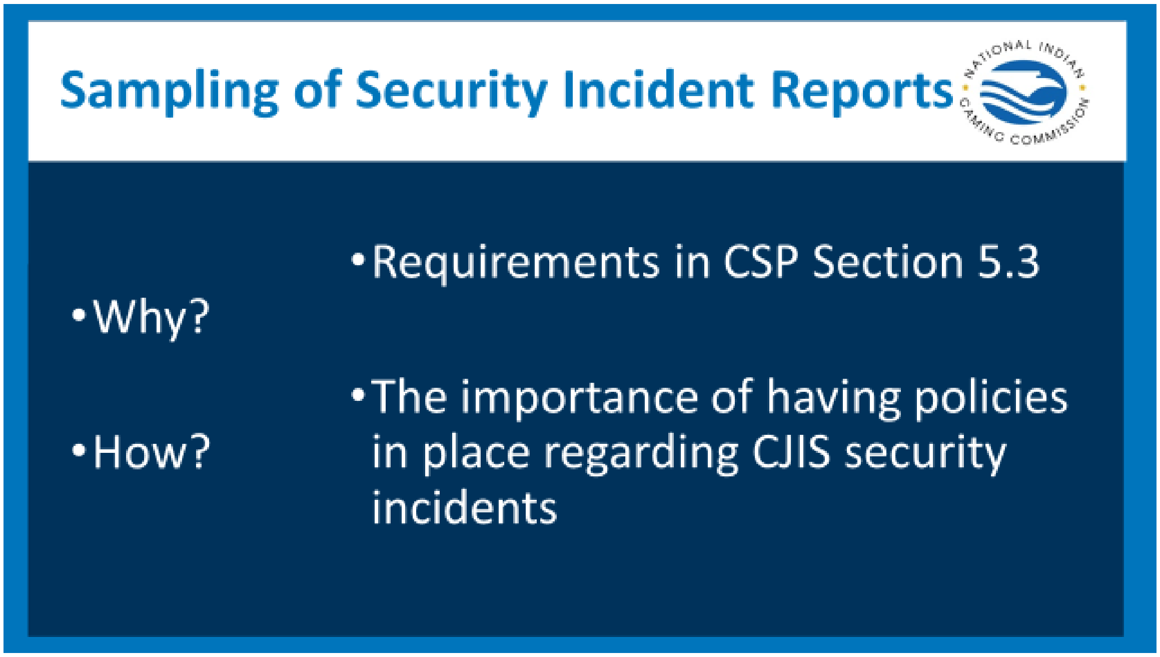
Security Awareness Training

- Lvl 1 – CSP 5.2.1.1 – Incident Response
- Lvl 2 – CSP 5.2.1.2 – Media Protection, Social Engineering
- Lvl 3 – CSP 5.2.1.3 – Access control, Passwords
- Lvl 4 – CSP 5.2.1.4 – IT Staff, INCLUDING Outsourced Staff
- LASO Training – Responsibilities, Audit Details

There are 5 types of training. Each one has slightly different responsibilities and knowledge that they require as outlined in the CSP.

Free training materials are available on the NIGC website.

NOTES

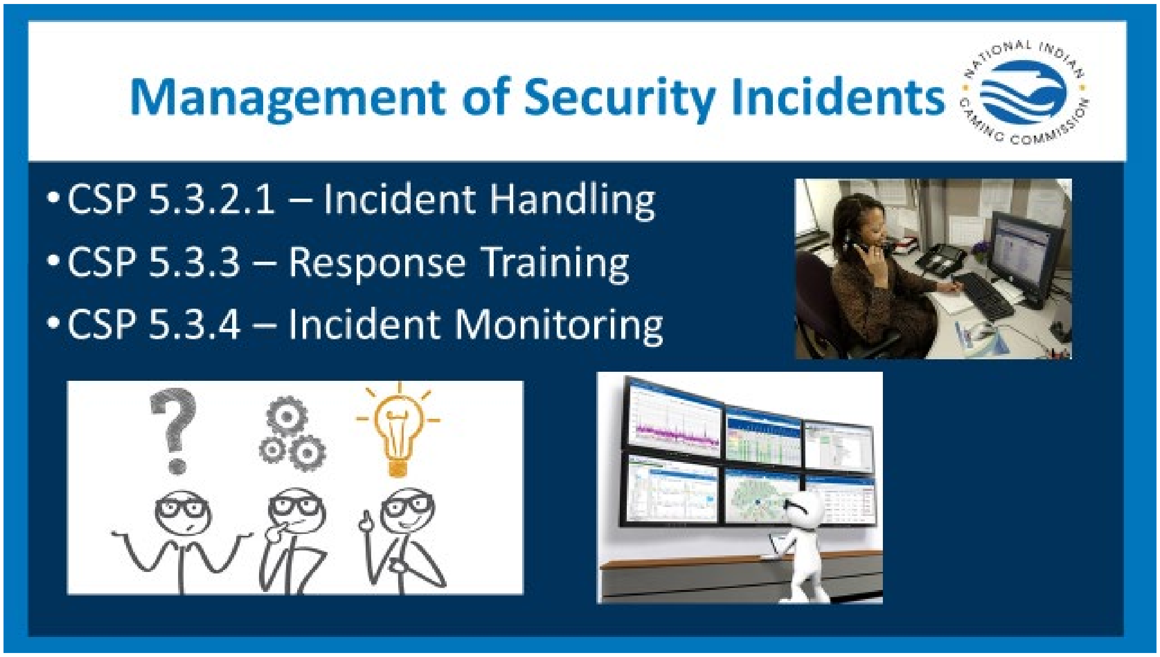

NATIONAL INDIAN GAMING COMMISSION

Sampling of Security Incident Reports

- Why?
- How?

- Requirements in CSP Section 5.3
- The importance of having policies in place regarding CJIS security incidents

NOTE:



Management of Security Incidents

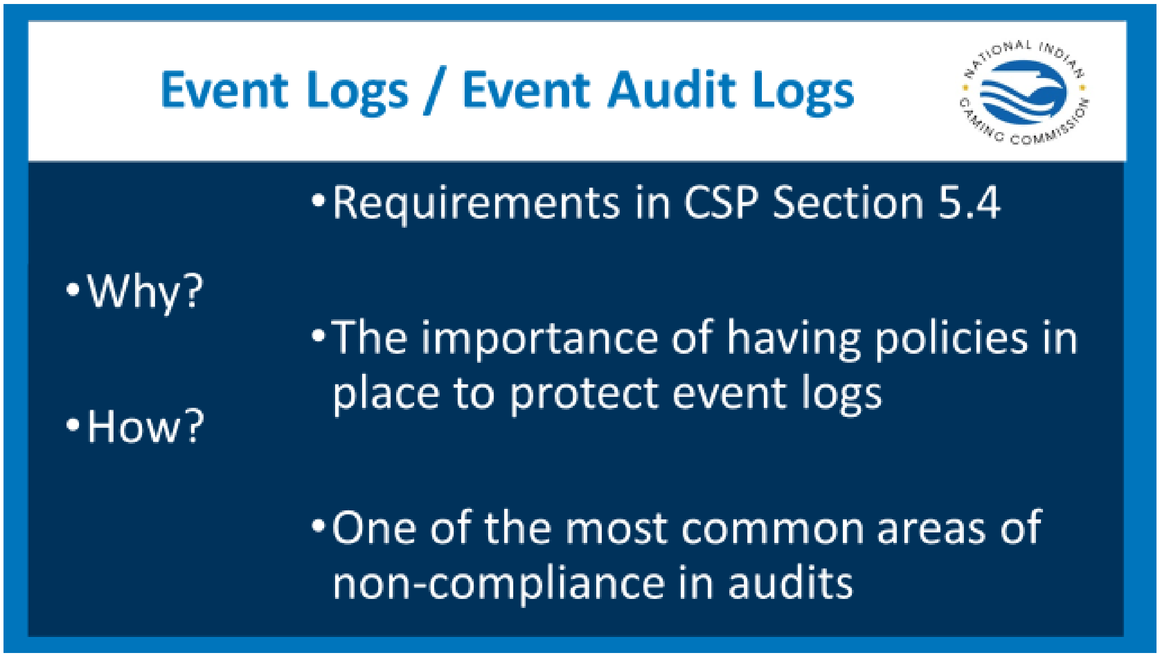
- CSP 5.3.2.1 – Incident Handling
- CSP 5.3.3 – Response Training
- CSP 5.3.4 – Incident Monitoring

The CSP has requirements regarding security incidents. Specific policies need to be in place that addresses incidents.

Policies and documentation of response training to various types of incidents should be completed. This is important so that staff knows how to respond and who to call in response to these incidents.

This is a common finding for MICS and a common non-compliant area for CJIS policies.

NOTES



Event Logs / Event Audit Logs

- Why?
- How?

- Requirements in CSP Section 5.4
- The importance of having policies in place to protect event logs
- One of the most common areas of non-compliance in audits

NOTES

____

____

____

____

____

____

____

____

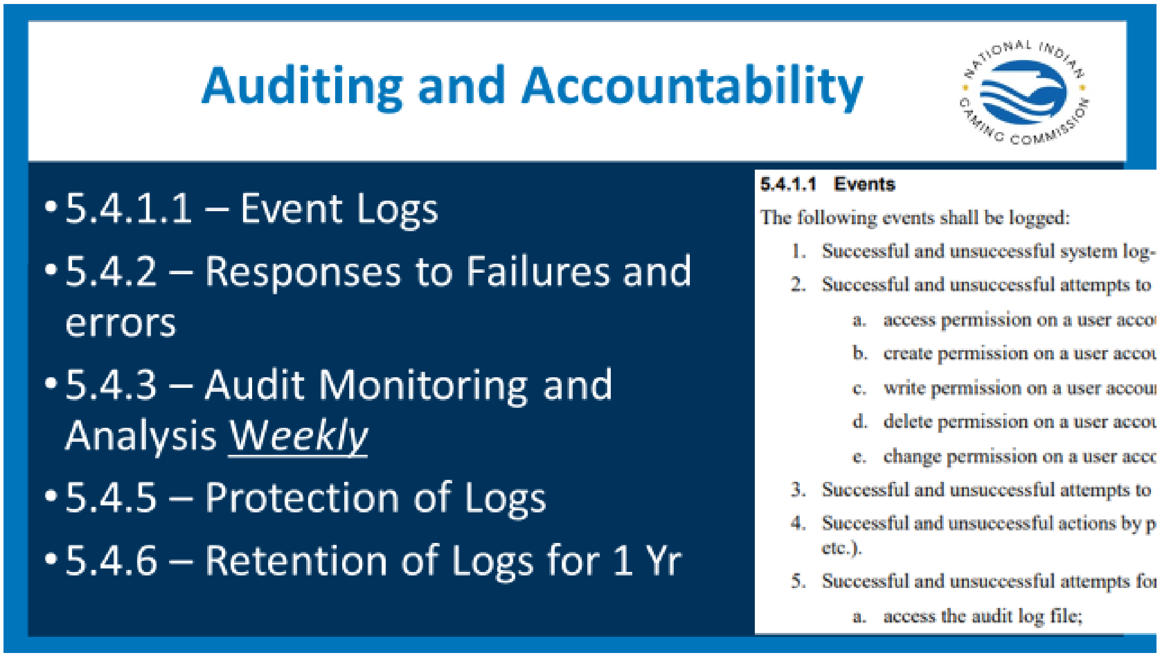
____

____

____

____

____



Auditing and Accountability

- 5.4.1.1 – Event Logs
- 5.4.2 – Responses to Failures and errors
- 5.4.3 – Audit Monitoring and Analysis *Weekly*
- 5.4.5 – Protection of Logs
- 5.4.6 – Retention of Logs for 1 Yr

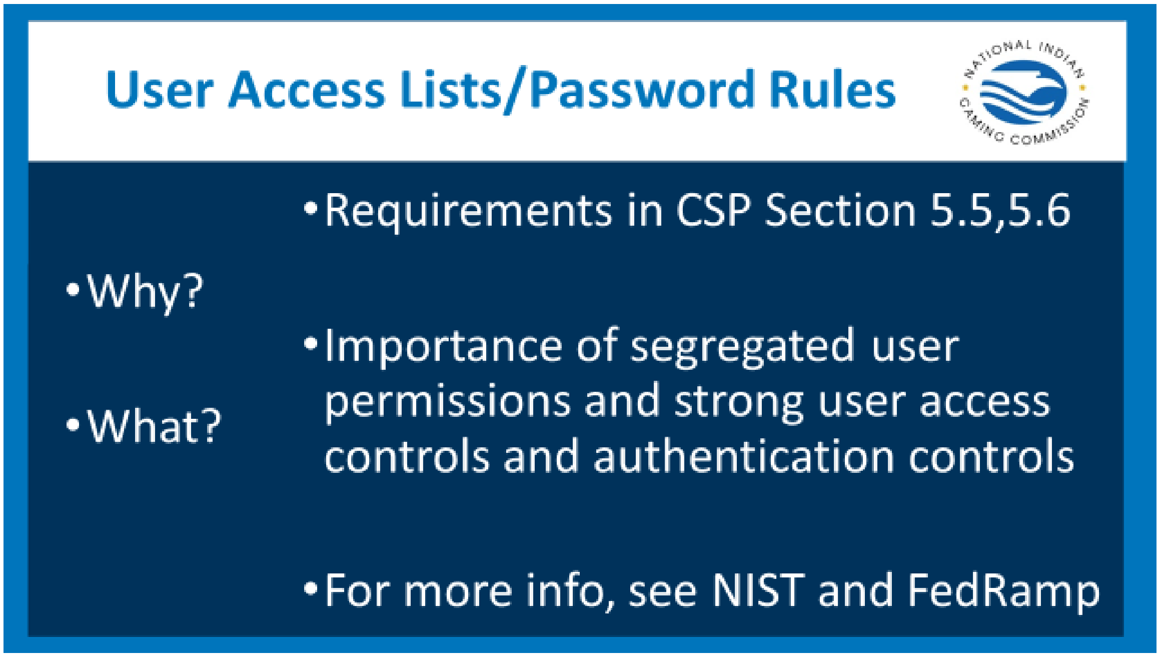
5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-
2. Successful and unsuccessful attempts to
   a. access permission on a user acco
   b. create permission on a user accou
   c. write permission on a user accou
   d. delete permission on a user accou
   e. change permission on a user acc
3. Successful and unsuccessful attempts to
4. Successful and unsuccessful actions by p etc.).
5. Successful and unsuccessful attempts fo
   a. access the audit log file;

The CSP has requirements regarding Event record keeping and Event logging as well as weekly audits of these event logs.

NOTES



User Access Lists/Password Rules

- Why?
- What?

- Requirements in CSP Section 5.5,5.6
- Importance of segregated user permissions and strong user access controls and authentication controls
- For more info, see NIST and FedRamp

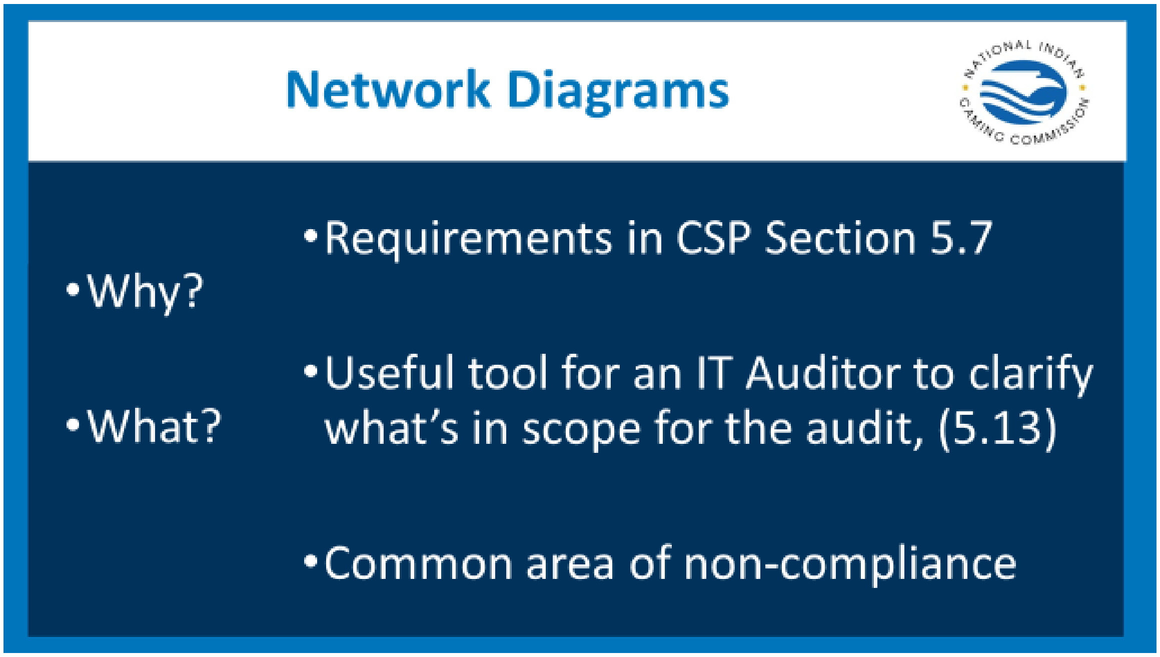
NOTES

NATIONAL INDIAN GAMING COMMISSION
USER
GROUP
CAUTION
P@$5w0rD
RSA SecurID

Access Control/Authentication

- 5.5.2.4 – Access Control Mechanisms
- 5.5.3 – Unsuccessful Login Attempts
- 5.5.4 – System Use Notification
- 5.6.2.1 – Passwords, PIN, One-Time-Passwords
- 5.6.3 – Authenticators, MFA/2FA

NOTES

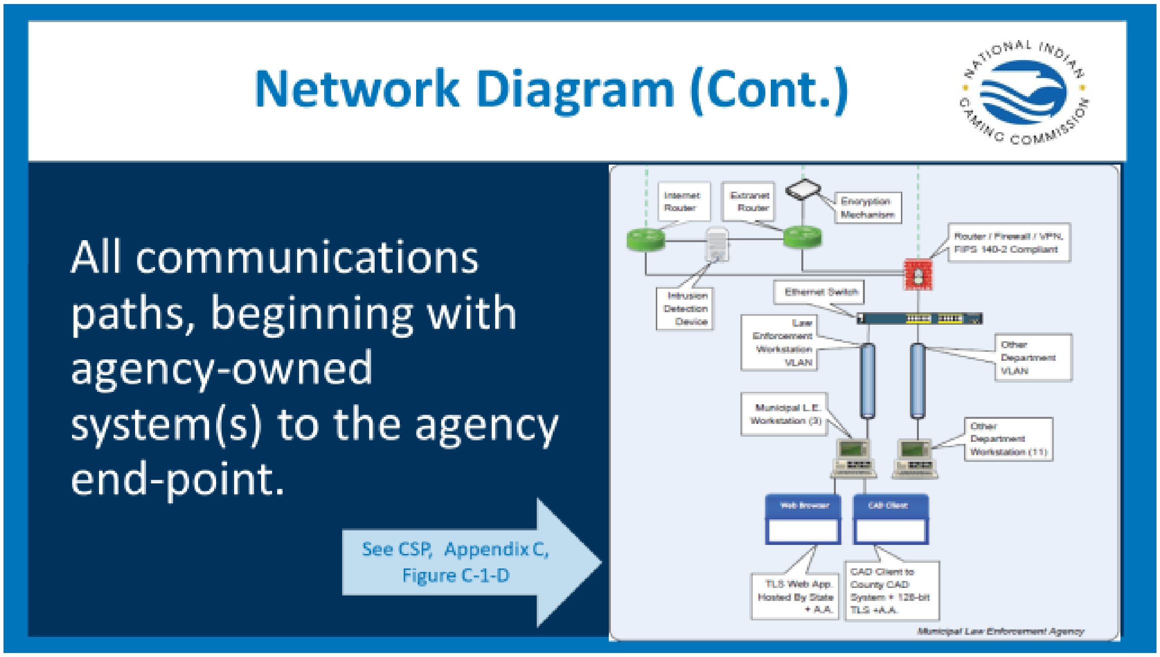


Network Diagrams

- Why?
- What?

- Requirements in CSP Section 5.7
- Useful tool for an IT Auditor to clarify what's in scope for the audit, (5.13)
- Common area of non-compliance

NOTES



Network Diagram (Cont.)

All communications paths, beginning with agency-owned system(s) to the agency end-point.

See CSP, Appendix C, Figure C-1-D

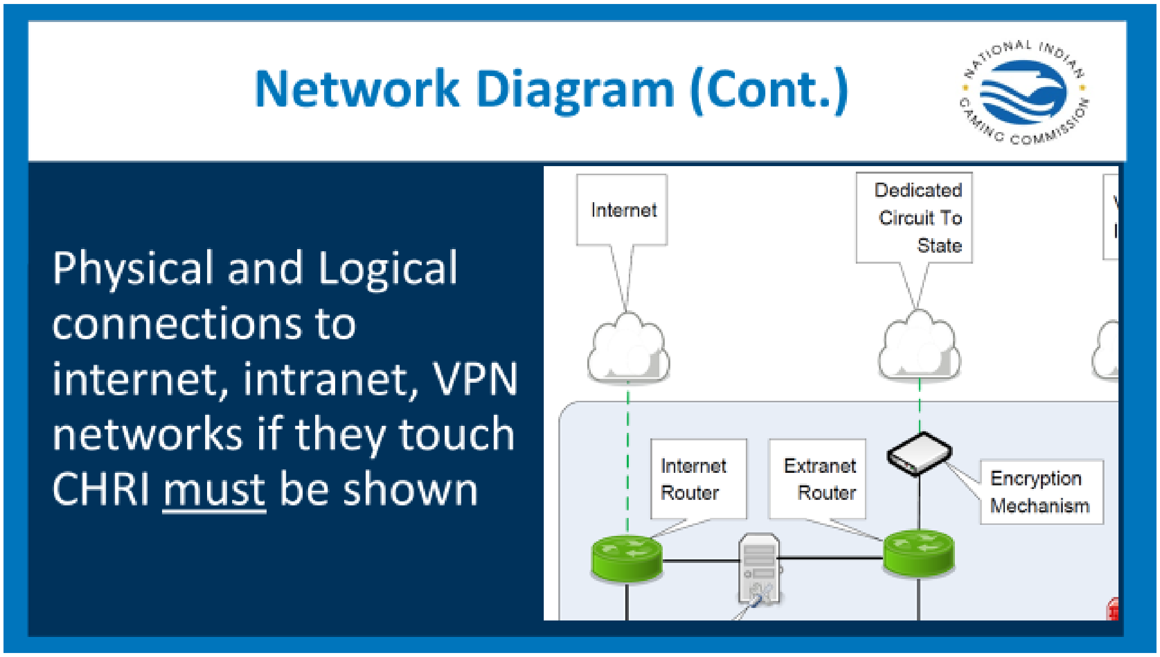
NATIONAL INDIAN GAMING COMMISSION
Internet Router
Extranet Router
Encryption Mechanism
Router / Firewall / VPN, FIPS 140-2 Compliant
Intrusion Detection Device
Ethernet Switch
Law Enforcement Workstation VLAN
Other Department VLAN
Municipal L.E. Workstation (3)
Other Department Workstation (11)
Web Browser
CAD Client
TLS Web App. Hosted By State + A.A.
CAD Client to County CAD System + 128-bit TLS +A.A.
Municipal Law Enforcement Agency

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.



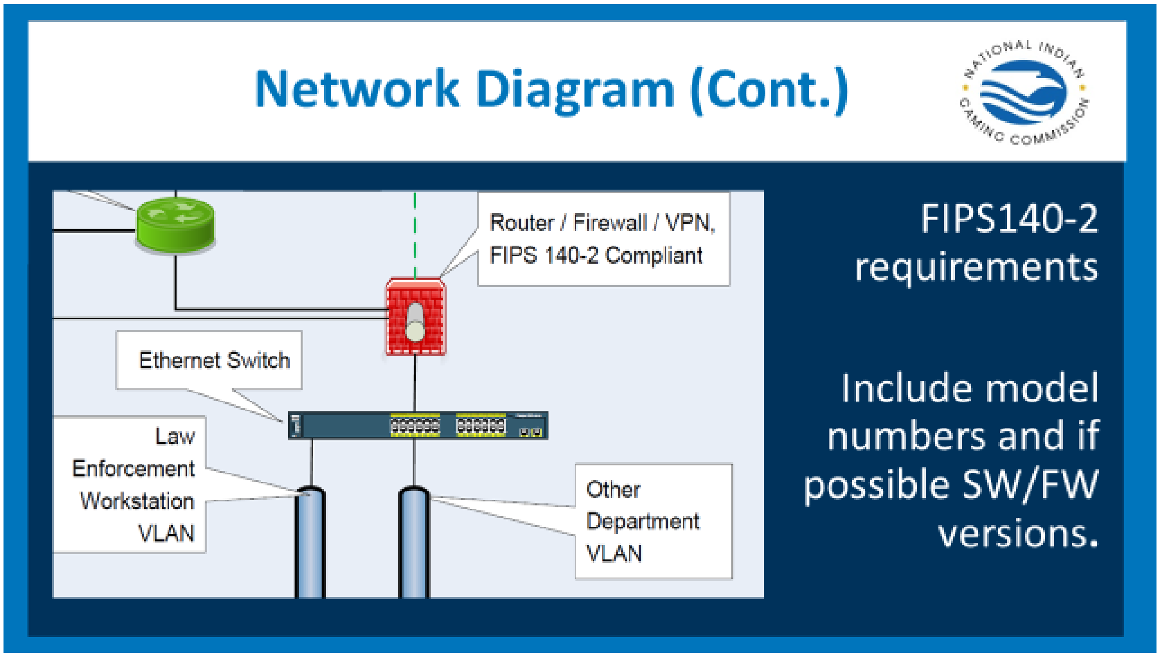
Network Diagram (Cont.)

Physical and Logical connections to internet, intranet, VPN networks if they touch CHRI <u>must</u> be shown

5.7.1.2 Network Diagram
The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.



Network Diagram (Cont.)

NATIONAL INDIAN GAMING COMMISSION
Router / Firewall / VPN, FIPS 140-2 Compliant
Ethernet Switch
Law Enforcement Workstation VLAN
Other Department VLAN

FIPS140-2 requirements

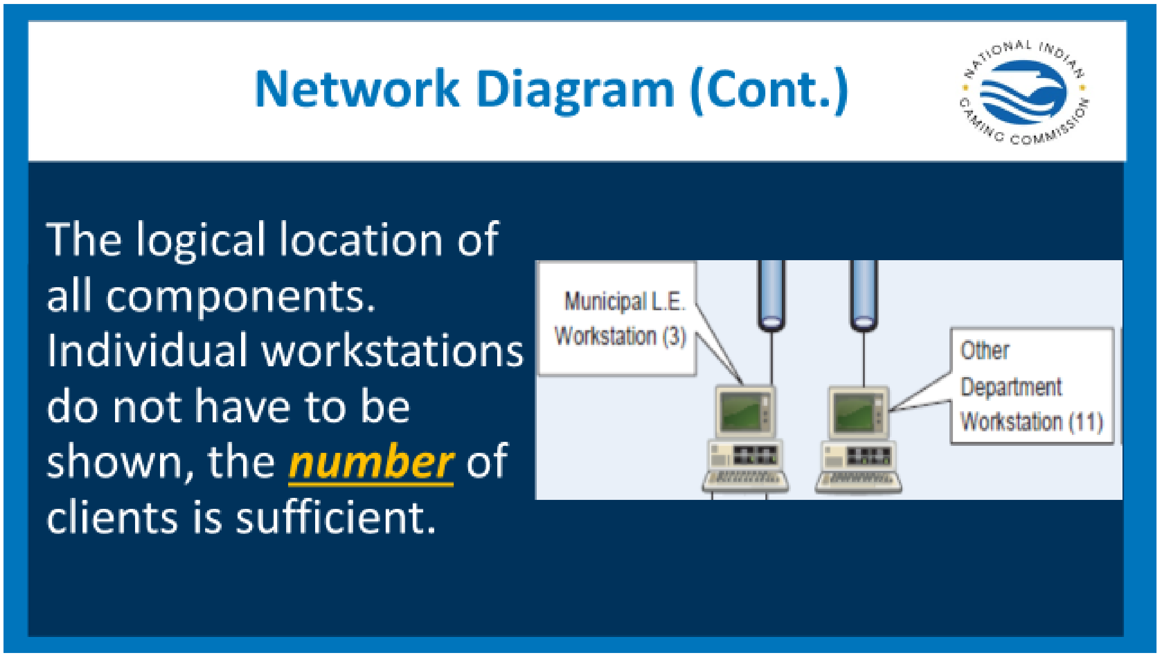
Include model numbers and if possible SW/FW versions.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

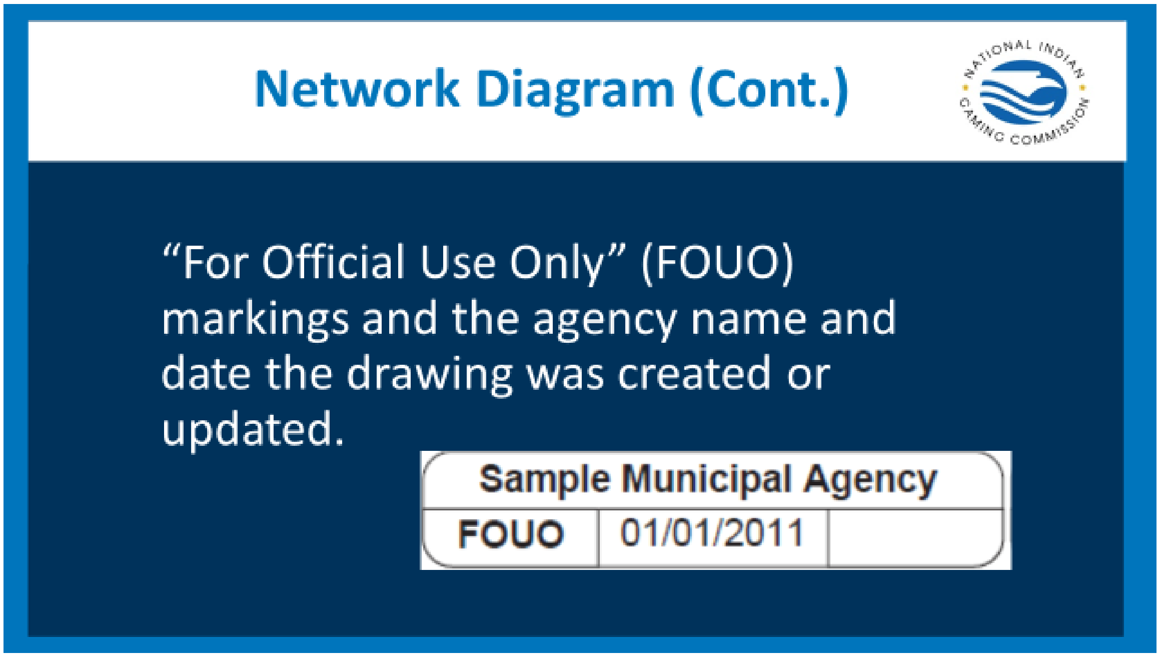
1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.



Network Diagram (Cont.)

The logical location of all components. Individual workstations do not have to be shown, the ***number*** of clients is sufficient.

NOTES



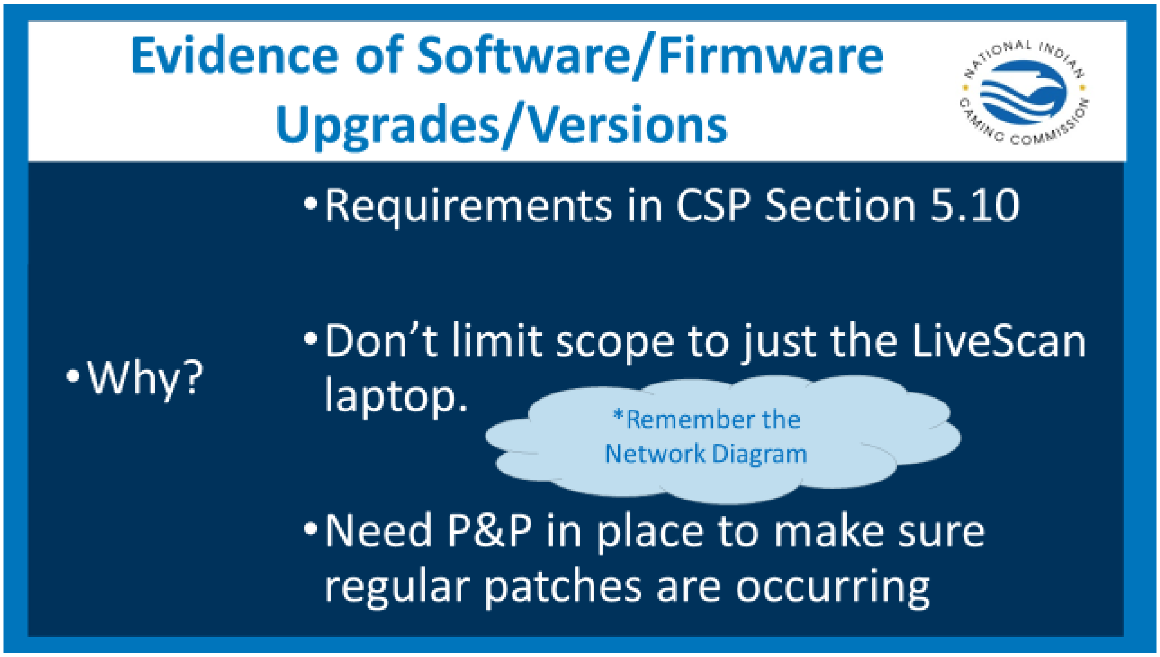
Network Diagram (Cont.)

NATIONAL INDIAN GAMING COMMISSION

“For Official Use Only” (FOUO) markings and the agency name and date the drawing was created or updated.

Sample Municipal Agency		
FOUO	01/01/2011	

NOTES



Evidence of Software/Firmware Upgrades/Versions

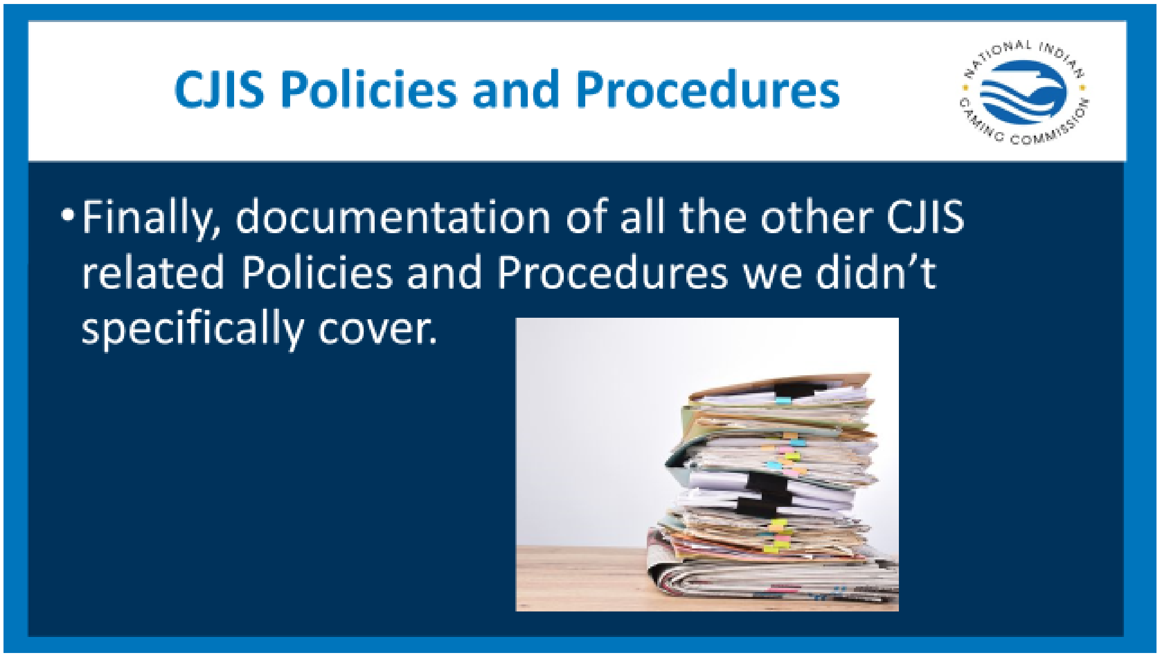
- Why?

- Requirements in CSP Section 5.10
- Don’t limit scope to just the LiveScan laptop.

*Remember the Network Diagram

- Need P&P in place to make sure regular patches are occurring

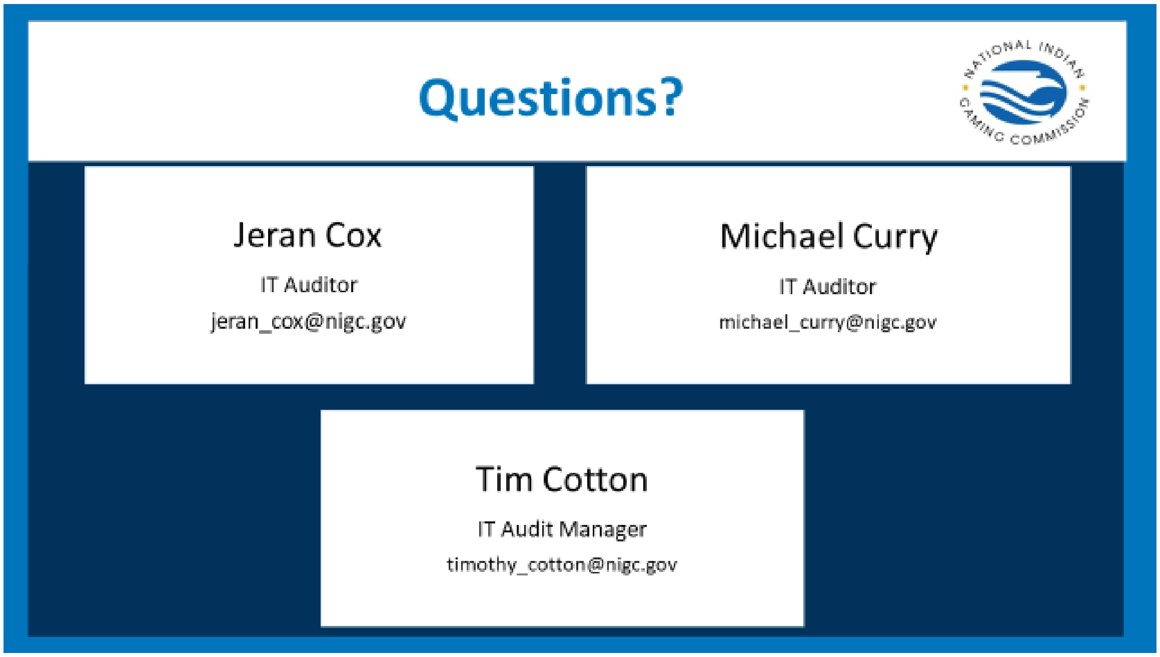
NOTES



CJIS Policies and Procedures

- Finally, documentation of all the other CJIS related Policies and Procedures we didn't specifically cover.

NOTES



Questions?

Jeran Cox

IT Auditor

jeran_cox@nigc.gov

Michael Curry

IT Auditor

michael_curry@nigc.gov

Tim Cotton

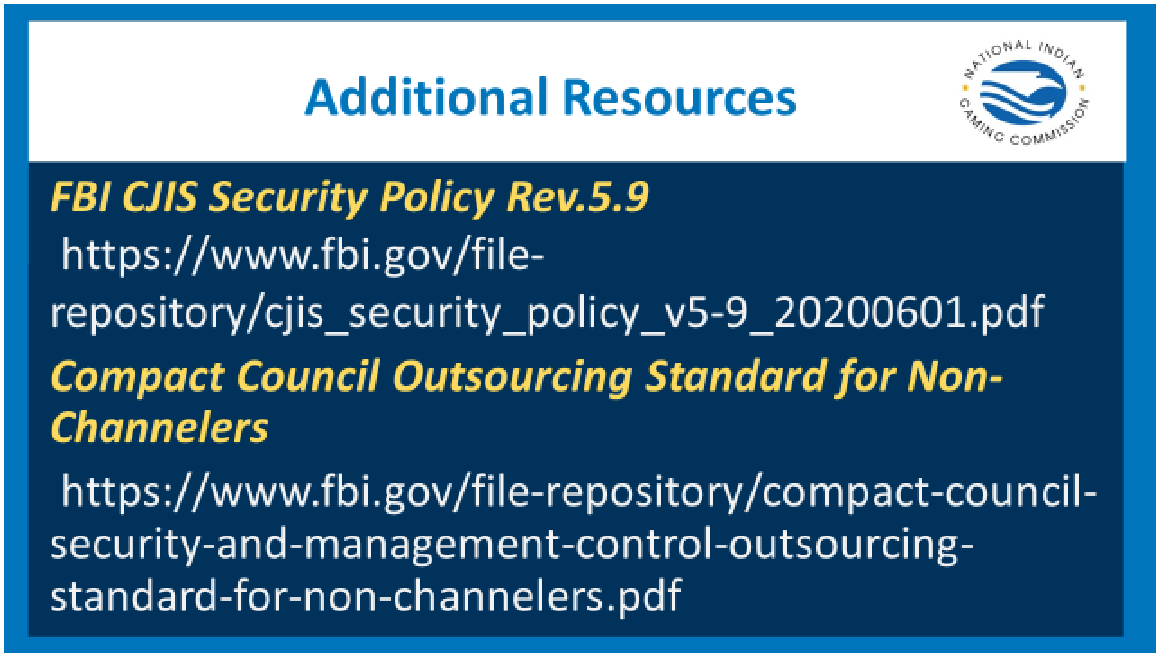
IT Audit Manager

timothy_cotton@nigc.gov

Thank you for your participation and attending 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!

NIGC Training can be reached at traininginfo@nigc.gov



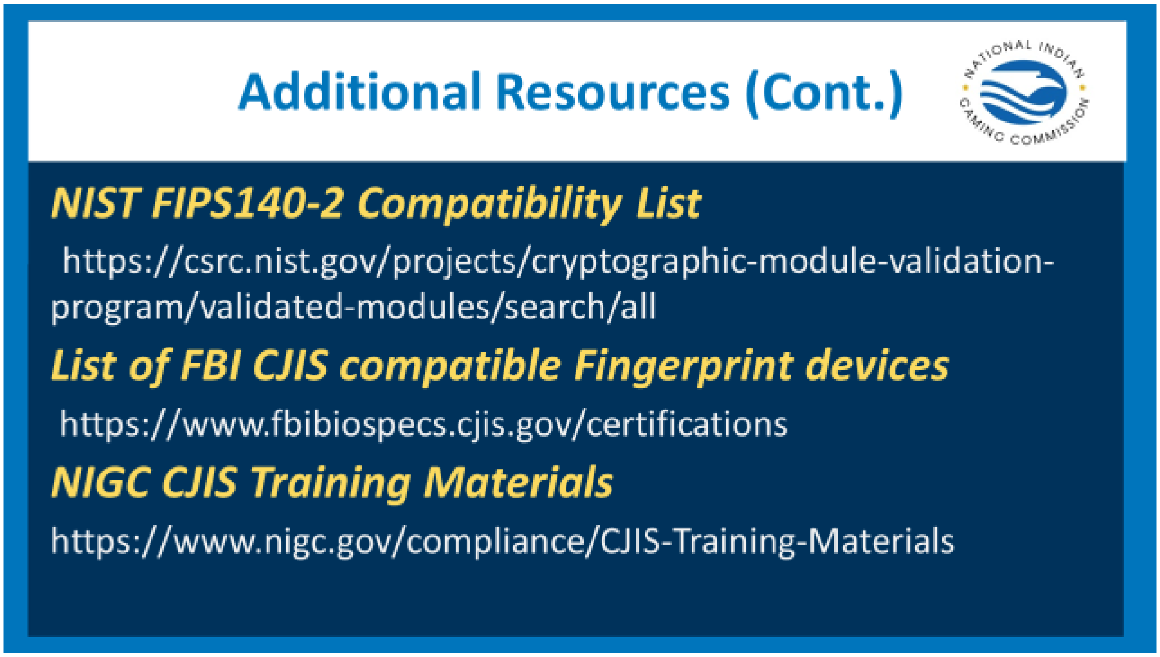
Additional Resources

FBI CJIS Security Policy Rev.5.9

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

Compact Council Outsourcing Standard for Non-Channelers

https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf



Additional Resources (Cont.)

NIST FIPS140-2 Compatibility List

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

List of FBI CJIS compatible Fingerprint devices

https://www.fbibiospecs.cjis.gov/certifications

NIGC CJIS Training Materials

https://www.nigc.gov/compliance/CJIS-Training-Materials