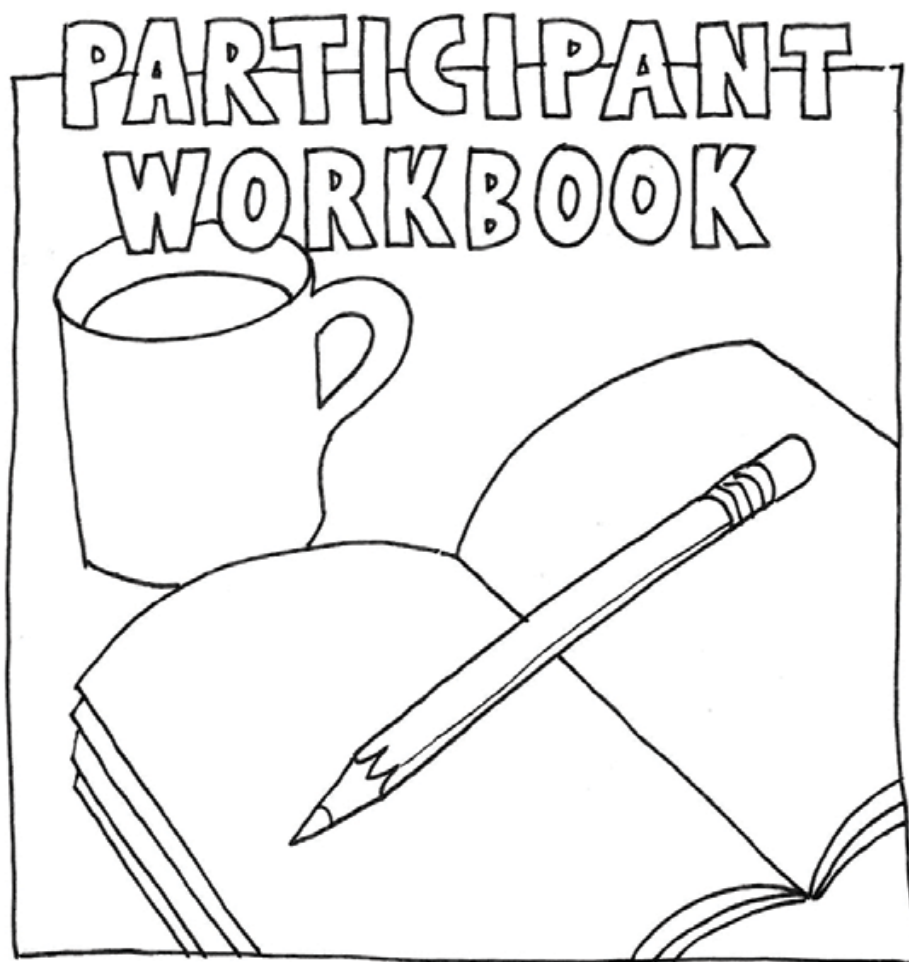




IT Boot Camp



CJIS IT Security Audit Overview

PART 1



NOTES

Part I - Training Objectives



- NIGC Fingerprint Processes Review
- Methods of Safeguarding CHRI and staying CJIS Compliant
- Identify Different CHRI locations
- High level NIGC CJIS IT Security Audit steps

NOTES

[illegible]

Part I - Training Objectives

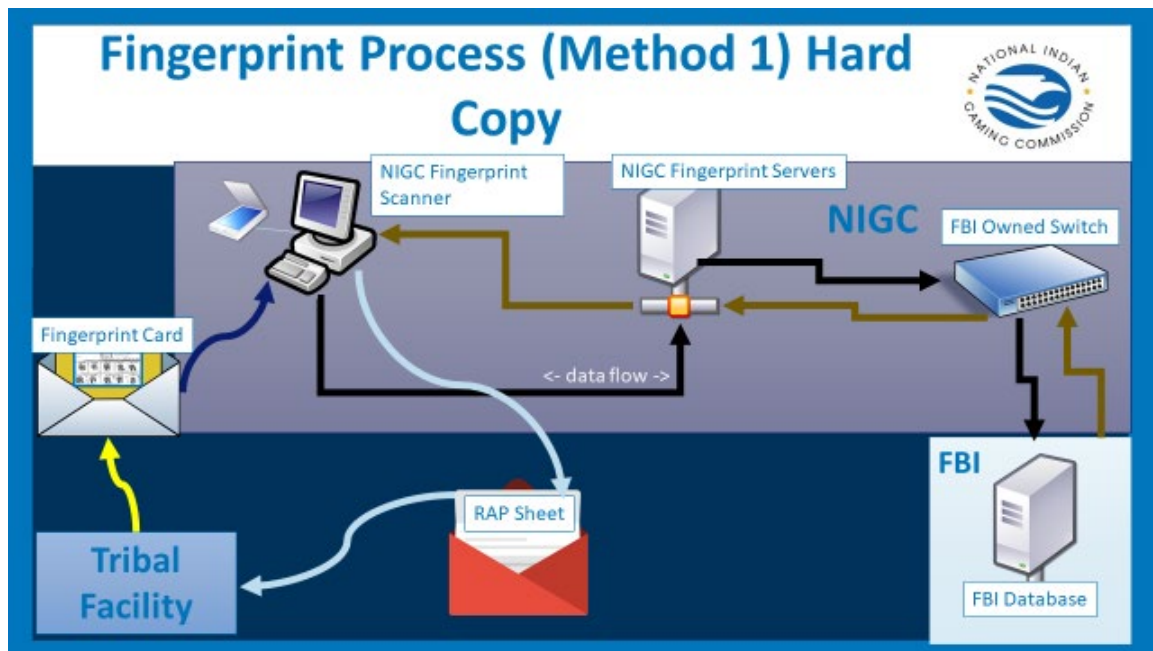


- NIGC Fingerprint Processes Review
- Methods of Safeguarding CHRI and staying CJIS Compliant
- Identify Different CHRI locations
- High level NIGC CJIS IT Security Audit steps

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

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

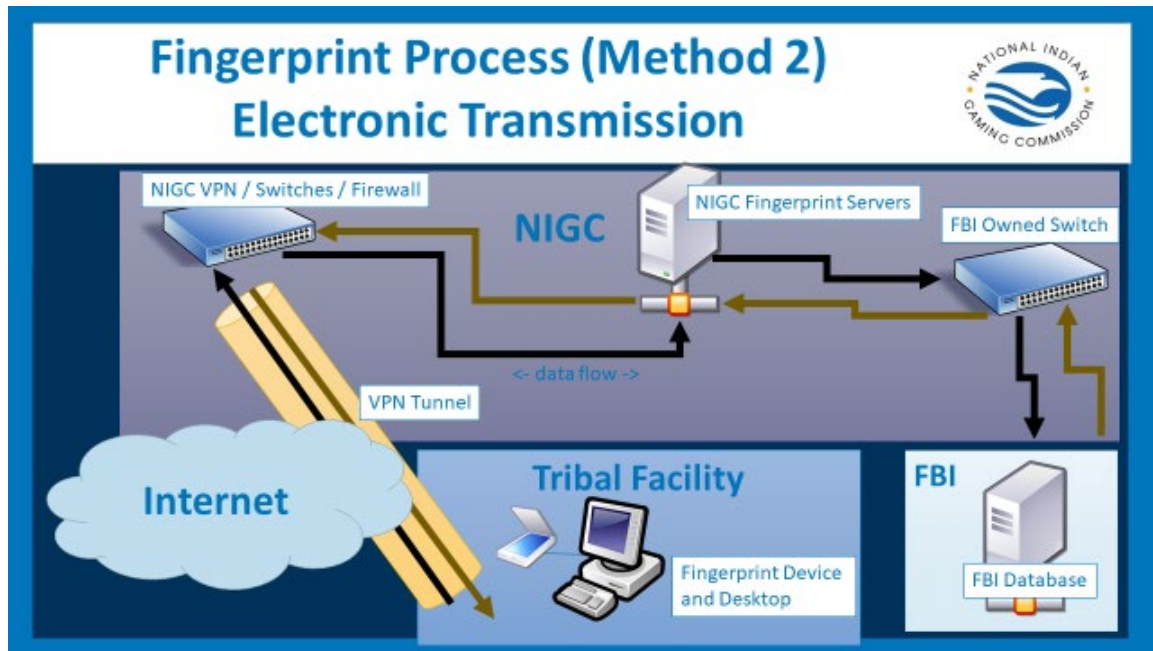


[Link to a list of FBI CJIS compatible Fingerprint devices.](#)

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

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

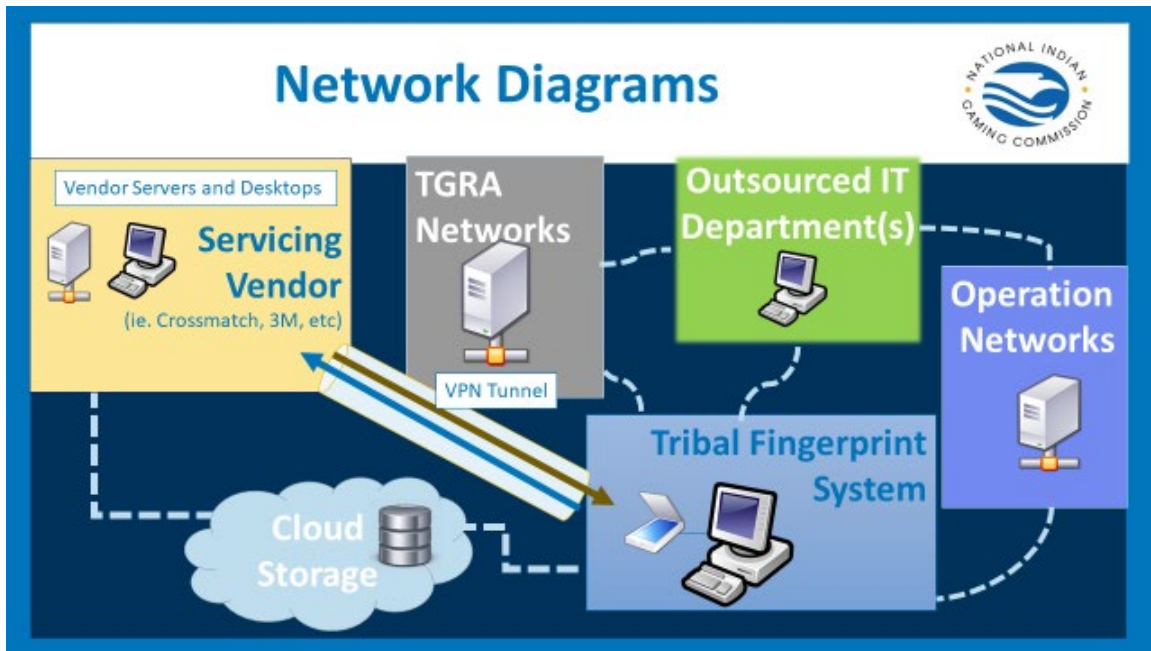


EBTS – Electronic Biometric Transmission Specification

- This is the most common method of usage.

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



While many fingerprint systems are configured to be as isolated as possible from other networks, they are typically housed within and have some level of connectivity to the TGRA office networks.

It is not uncommon for the fingerprint system to be somehow connected to various operational networks.

These connections to the TGRA and Operations networks by themselves are not necessarily out of compliance.

However, one must keep in mind who is handling the IT service contracts for each of those networks, (Fingerprint, TGRA, Operations).


NOTES

CJIS Security Policy and ITS Audits

FBI CJIS Security Policy Rev.5.9, - 253 Pages, 13 Sections
CJIS ITS Audits with ~160+ checklist items

5.1 Information Exchange Agreements	5.7 Configuration Management
5.2 Security Awareness Training	5.8 Media Protection
5.3 Incident Response	5.9 Physical Protection
5.4 Auditing and Accountability	5.10 System and Communications Protection and Information Integrity
5.5 Access Control	5.11 Formal Audits
5.6 Identification and Authentication	5.12 Personnel Security
	5.13 Mobile Devices

Where to Start?



References:

FBI CJIS Security Policy Rev.5.9

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

- 5.1 Information Exchange Agreements*
- 5.2 Security Awareness Training*
- 5.3 Incident Response*
- 5.4 Auditing and Accountability*
- 5.5 Access Control*
- 5.6 Identification and Authentication*
- 5.7 Configuration Management*
- 5.8 Media Protection*
- 5.9 Physical Protection*
- 5.10 System and Communications Protection and Information Integrity*
- 5.11 Formal Audits*
- 5.12 Personnel Security*
- 5.13 Mobile Devices*

CJIS Security Policy and IT Security Audits



- *Where is CHRI Stored?*
- *Who has Access to CHRI?*
- *How is CHRI Protected During Storage?*
- *How is CHRI Protected During Transit?*

CJIS Security
goals in fewer
than 130
characters...



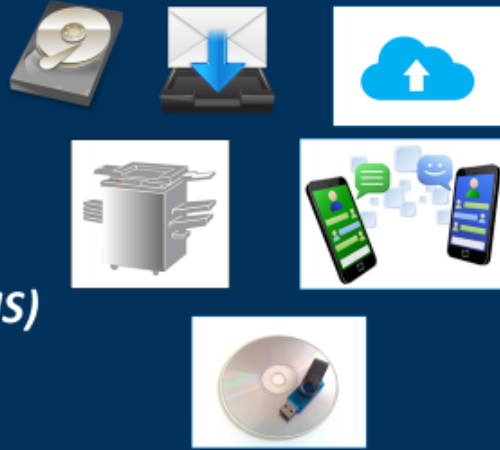
NOTE:_____

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



Where is CHRI Stored?

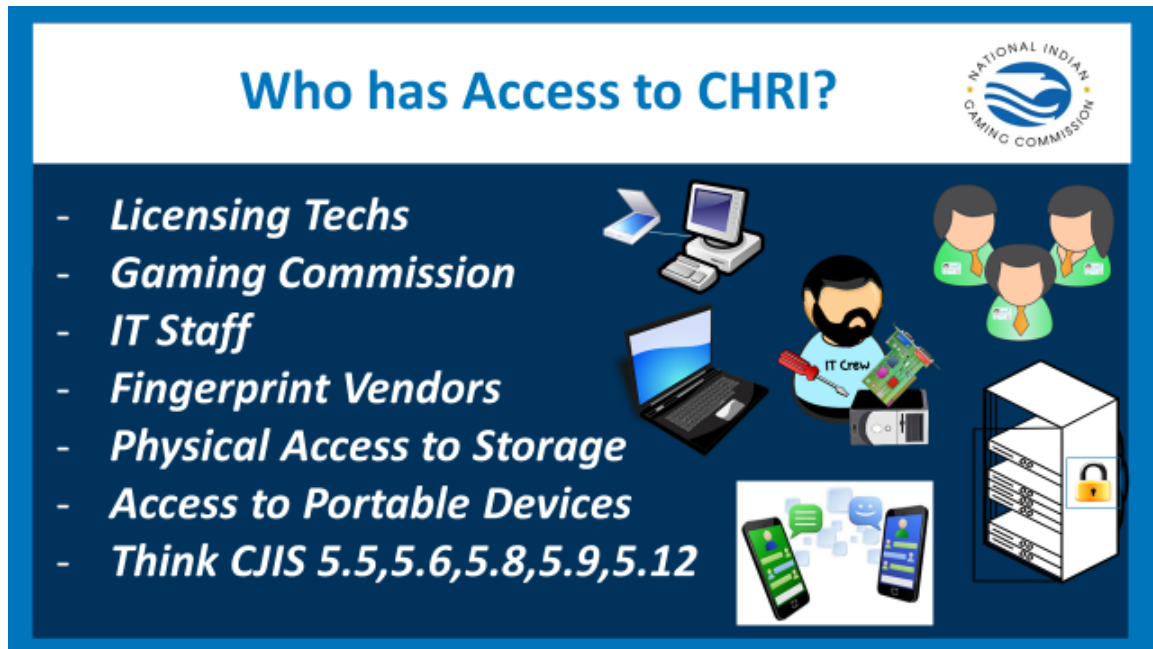
- *Local Hard Drive*
- *Software's Email Inbox*
- *Vendor's Cloud Service*
- *Hard Copies, Print Outs*
- *Photocopies*
- *Smartphone, (photos, SMS)*
- *Media, (USB, CD)*
- *Think CJIS 5.8,5.9,5.10*



- 5.8 Media Protection, Sanitation, disposal
- 5.9 Physical protection
- 5.10 System and Communications Protection and Information Integrity

NOTES

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.




- 5.5 Access Control
- 5.6 Identification and Authentication
- 5.8 Media Protection, Sanitation, disposal
- 5.9 Physical protection
- 5.12 Personnel security

NOTES

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slight shadow on the right side, suggesting it's resting on a surface.

How is CHRI Protected During Storage?



- *Locks on Doors*
- *Locks on Cabinets*
- *Local File Encryption*
- *Local Disk Encryption*
- *Network or Cloud Storage*
- *Types of Devices*
- *Think CJIS 5.5,5.6,5.8,5.9,5.12*



- 5.5 Access Control
- 5.6 Identification and Authentication
- 5.8 Media Protection, Sanitation, disposal
- 5.9 Physical protection
- 5.12 Personnel security

NOTES

How is CHRI Protected During Transit?

- *Over a VPN*
- *Over a Network*
- *Via Paper*
- *Via Email, fax*
- *Via Phone*
- *Via Teleconference*
- *Think CJIS 5.9, 5.10, 5.13*



The collage includes several icons: a network diagram showing three laptops (labeled A, B, and C) connected to a central server; a cloud labeled 'VPN' connected to two desktop computers; a smartphone; an orange sticky note with a blue pushpin; a blue envelope icon; and a blue silhouette of two people in a teleconference with speech bubbles.

5.9 Physical Protection

5.10 System and Communications Protection and Information Integrity

5.13 Mobile devices

NOTES

[illegible]

CJIS IT Security Audit- Initial Steps

1 - Announcement Letter

2 - Mail Out

3 - Checklist

Date:

(To be completed later)
Tribal Gaming Regulatory Authority
(Outgoing Address)

RE: CTS (Information Technology) Security Audit Notification Letter

Dear (Local Agency Security Officer):

This correspondence is to respectfully confirm the telephone conference on (7/8/88) and the National Indian Gaming Commission (NIGC) on (10/13/1) regarding IT, 347, C.T. CTS) to conduct a Criminal Justice Information System and Technology Security Audit (CJIS ITS Audit). The CTS ITS Audit assumes using FBI's CTS Security Policy, reviewing the information technology systems, procedures, and rights subsequent criminal justice system information. Specifically, this CTS ITS Audit focuses on unclassified systems, systems and does CJIS, system administration and protection, confidentiality of Noncriminal Justice Functions and audit thereof, information protection, systems administration, and CTS ITS Audit assumes compliance with the CTS Security Policy, the NIGC CTS Information of Understanding (MOT), and NIGC policies. Importantly, this is done the NIGC CTS ITS Audit notification letter has been scheduled with you for a date and time.

The purpose of the CTS ITS Audit is to verify the Tribal Gaming Regulator (TGR) and individual user compliance with the following:

- Applicable laws, regulations, and requirements of the FBI CTS Security Policy;
- The Tribal CTS ITS Audit into the NIGC; and
- All internal NIGC, applicable policies, including the NIGC Non-criminal Justice Functions.

The CTS Security Policy obligates the CTS Systems Agency (CSA)—the NIGC

National Indian Gaming Commission

(NIGC)

Information Technology Security Audit

CJIS Policy Policy Area 1	Policy Area Information Exchange Agreements	Requirement
5.1	Information Exchange Agreements	Does the information shared through communications systems and information systems and communications medium: vital to the system's fully understanding and agreeing to a set of standards? (Refer to NIGC MOT document) Prior to exchanging CI, have the agencies put forth in place that specify security controls? The exchange information may take several forms including electronic messages, web services, facsimile, hard copy, and systems sending, receiving and storing CI.
5.1.1	Information Exchange	Does the information exchange agreements outline responsibility, and data ownership between external parties? Information exchange agreements sharing CI data that is sent to and/or received from specify the security controls and conditions described document. Are the information exchange agreements supported documentation committing both parties to the information exchange? As described in subsequent different agreements and policies apply, depending

How the NIGC CJIS IT Security Audit proceeds.

- Announcement letter is sent out
- The NIGC IT Security Audit Correspondence Questionnaire is sent along with a copy of the IT Security Audit checklist.

NOTES

[illegible]

Audit Documentation Request



- ***Outsourcing Agreements / 90 day Audits (5.1)***
- ***Personnel Lists / LASO and Training Records (5.2)***
- ***Sampling of Security Incident Reports (5.3)***
- ***Event Logs / Event Log Audits (5.4)***
- ***User Access Lists, Password Rules, etc. (5.5, 5.6)***

Along with the items in the previous slide, a listing of documents will be requested. Review of these documents and the answers to the questionnaire will provide some answers to the items in the audit checklist.

Note: This list is not exhaustive and additional documents may need to be requested/reviewed as the audit progresses.

NOTES

[illegible]

Audit Documentation Request (Cont.)

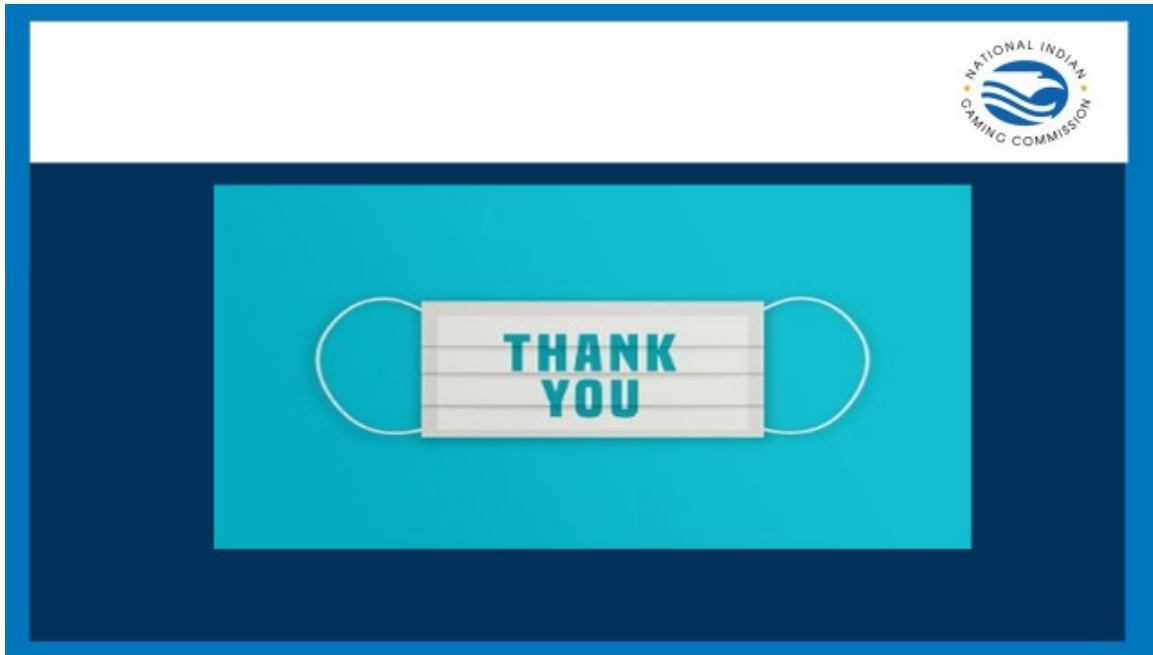


- **Network Diagrams (5.7, 5.10, 5.13)**
- **Media Destruction / Sanitization logs (5.8, 5.9)**
- **Evidence of Software/Firmware Upgrades/Versions (5.10)**
- **Personnel Security Policies, Termination Records (5.12)**
- **All other P&Ps for CSP 5.1 through 5.13**

Note: This list is not exhaustive and additional documents may need to be requested/reviewed as the audit progresses.

NOTES

[illegible]



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!

See you next session for Part II.

NIGC Training can be reached at traininginfo@nigc.gov