




National Indian Gaming Commission


CJIS

NIGC Fingerprint Process



Training Objectives

- NIGC Fingerprint Processes Review



Training Objectives

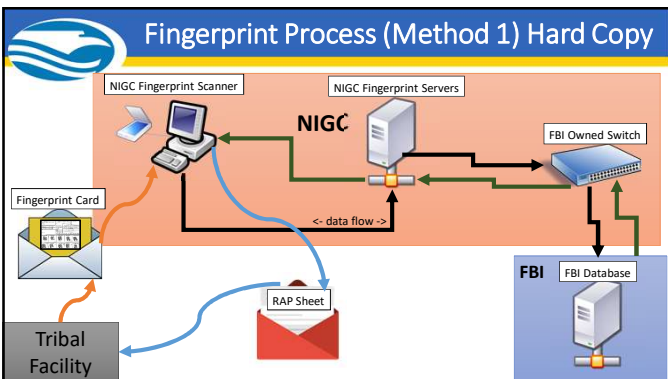
- NIGC Fingerprint Processes Review
- Methods of Safeguarding CHRI and staying CJIS Compliant

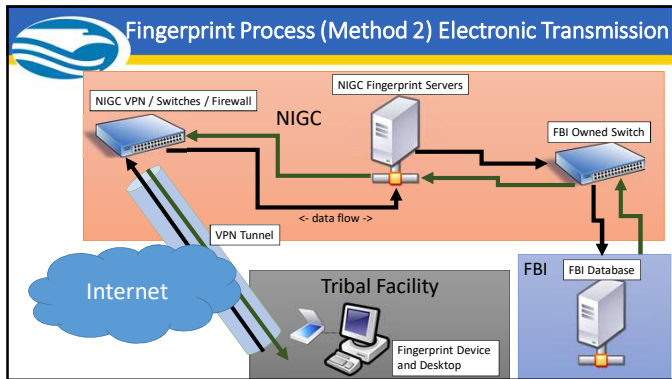
Training Objectives

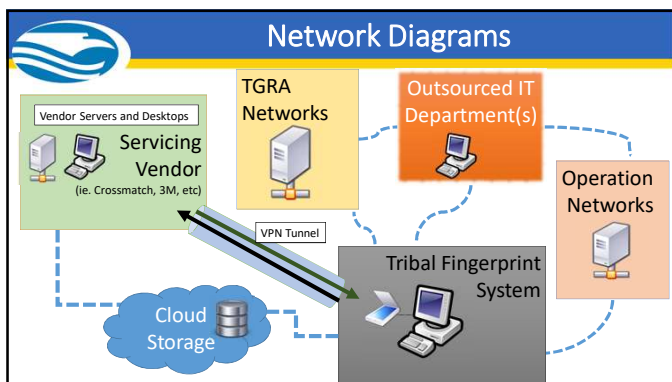
- NIGC Fingerprint Processes Review
- Methods of Safeguarding CHRI and staying CJIS Compliant
- Identify Different CHRI locations

Training Objectives

- NIGC Fingerprint Processes Review
- Methods of Safeguarding CHRI and staying CJIS Compliant
- Identify Different CHRI locations
- Different types of Vendor Access, NCJA (Noncriminal Justice Administrator) Functions, and Non-Channeler Responsibilities







CJIS Security Policy and IT Security Audits

FBI CJIS Security Policy Rev.5.9
 - 253 Pages, 13 Sections – (5.1 through 5.13)
 - 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
5.5 Access Control	5.11 and Information Integrity
5.6 Identification and Authentication	5.11 Formal Audits
	5.12 Personnel Security
	5.13 Mobile Devices

TL;DR

Where to Start?


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... 

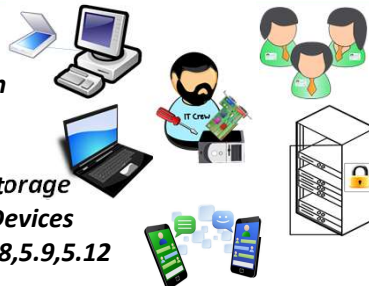
Where is CJIS Stored?

- **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**



Who has Access to CHRI?

- **Licensing Techs**
- **Gaming Commission**
- **IT Staff**
- **Fingerprint Vendors**
- **Physical Access to Storage**
- **Access to Portable Devices**
- **Think CJIS 5.5,5.6,5.8,5.9,5.12**

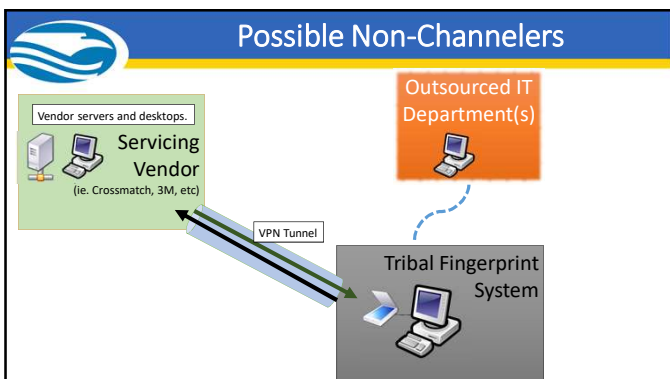



How is CHRI Protected During Storage?

- 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

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





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

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>
