


National Indian Gaming Commission



**Media and Physical Protection –  
Part 556 and 558 considerations**

---

---

---


---

---

---

---

---



Training Objectives

- Media and Physical Protection policy areas

---

---

---


---

---

---

---

---



Training Objectives

- Media and Physical Protection policy areas
- Shall statements

---

---

---


---

---

---

---

---

 Training Objectives

- Media and Physical Protection policy areas
- Shall statements
- Parts 556 and 558 as it relates to CHRI

---

---

---

---


---

---

---

---

U. S. Department of Justice  
Federal Bureau of Investigation  
*Criminal Justice Information Services Division*



**Criminal Justice Information Services (CJIS)  
Security Policy**

Version 5.9  
06/01/2020

CJISD-ITS-DOC-08140-5.9

---

---

---

---

---

---

---

---

What is CHRI?

---

---

---

---

---

---

---

---

## What is CHRI?

Criminal History Record Information (CHRI) means information collected by criminal justice agencies about individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.

---

---

---

---

---

---

---

---

## What is CHRI?

CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI. CHRI includes any media that contains it, such as: Letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables.

---

---

---

---

---

---

---

---

## What is CHRI?

Examples of CHRI potentially include: notice of results (NORs), investigative reports (IRs), licensing objection letters, and other summaries of CHRI. Updating the NOR to remove the FBI CHRI results can help eliminate summary CHRI.

---

---

---


---

---

---

---

---

 **5.8 Media Protection**

Media protection policy and procedures shall be documented and implemented.

Procedures shall be defined for securely handling, transporting and storing media.

---

---


---

---

---

---

---

 **5.8.1 Media Storage and Access**

The agency shall securely store digital and physical media.

The agency shall restrict access to digital and physical media.

If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

---

---


---

---

---

---

---

 **5.8.2 Media Transport**

The agency shall protect and control digital and physical media during transport outside of controlled areas.

---

---

---

---

---

---

---



### 5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.

---

---

---

---

---

---

---

---



### 5.8.2.2 Physical Media in Transit

Physical media shall be protected at the same level as the information would be protected in electronic form.

---

---

---

---

---

---

---

---



### 5.8.3 Digital Media Sanitization/Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals.

Inoperable digital media shall be destroyed (cut up, shredded, etc.).

---

---

---

---

---

---

---

---



### 5.8.3 Digital Media Sanitization/Disposal

The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media.

Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

---

---

---

---

---

---

---

---



### 5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures.

Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals.

---

---

---

---

---

---

---

---



### 5.8.4 Disposal of Physical Media

Physical media shall be destroyed by shredding or incineration.

Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

---

---

---


---

---

---

---

---

 5.9 Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

---

---

---


---

---

---

---

---

 5.9.1 Physical Secure Location



---

---

---


---

---

---

---

---

 5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

---

---

---

---

---

---

---

---



### 5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

---

---

---

---

---

---

---

---



### 5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

---

---

---

---

---

---

---

---



### 5.9.1.4 Access Control

The agency shall control physical access to information system distribution and **transmission** lines within the physically secure location.

---

---

---

---


---

---

---

---



 5.9.1.5 Access Control

The agency shall control physical access to information system devices that **display** CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

---

---

---


---

---

---

---

---

 5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

---

---

---


---

---

---

---

---

 5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).

The agency shall escort visitors at all times and monitor visitor activity.

---

---

---


---

---

---

---

---

 5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

---

---

---


---

---

---

---

---

 5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

---

---

---


---

---

---

---

---

 5.9.2 Controlled Area

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.

---

---

---


---

---

---

---

---



5.9.2 Controlled Area

3. Position information system devices and documents containing CJJ in such a way as to prevent unauthorized individuals from access and view.

4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJJ.

---

---

---

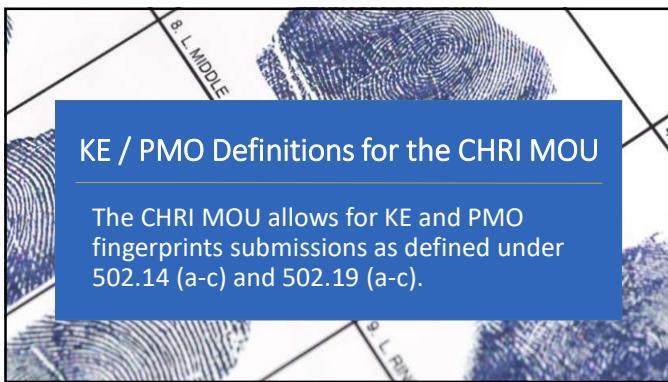
---

---

---

---

---



**KE / PMO Definitions for the CHRI MOU**

The CHRI MOU allows for KE and PMO fingerprints submissions as defined under 502.14 (a-c) and 502.19 (a-c).

---

---

---

---

---

---

---

---

**What is the CHRI MOU**




---

---

---

---

---

---

---

---

## What is the CHRI MOU

The CHRI MOU documents the agreed-upon responsibilities and functions of the parties with respect to the submission of noncriminal justice fingerprints for primary management officials (PMO) and key employees (KE) of Indian gaming enterprises, as defined by NIGC regulations, 25 C.F.R. §§ 502.14(a-c) and 502.19(a-c).

---

---

---

---

---


---

---

---

---

---



### How does CHRI impact Part 556.4?

**Fingerprints consistent with procedures adopted by a tribe according to §522.2(h) of this chapter.**

**556.4 Background Investigation**

A tribe shall perform a background investigation for each primary management official and for each key employee of a gaming operation:

(A) A tribe shall request from each primary management official and from each key employee all of the following information:

(1) Full name, other names used (oral or written), social security number(s), birth date, place of birth, citizenship, gender, all languages (spoken or written);

(2) Currently and for the previous five years, business and employment positions held, ownership interests in those businesses, business and residence addresses, and driver's license number(s);

(3) The names and current addresses of at least three personal references, including one personal reference who was acquainted with the applicant during each period of residence listed under paragraph (a) (2) of this section;

(4) Current business and residence telephone numbers;

(5) A description of any existing and previous business relationships with Indian tribes, including ownership interests in those businesses;

(6) A description of any existing and previous business relationships with the gaming industry generally, including ownership interests in those businesses;

(7) The name and address of any licensing or regulatory agency with which the person has filed an application for a license or permit related to gaming, whether or not such license or permit was granted;

(8) For each felony for which there is an ongoing prosecution or a conviction, the charge, the name and address of the court involved, and the date and disposition if any;

(9) For each misdemeanor conviction or ongoing misdemeanor prosecution (including minor traffic violations) within 10 years of the date of the application, the name and address of the court involved and the date and disposition;

---

---

---

---

---


---

---

---

---

---



### How can CHRI impact Part 556.6?

- Every known criminal charge within the last 10 years.
- Every felony conviction or any ongoing prosecution.

**556.6 Report to the Commission**

(a) When a tribe employs a primary management official or a key employee, the tribe shall maintain a complete application file containing the information listed under 556.4(a)(1) through (14).

(b) Before issuing a license to a primary management official or to a key employee, a tribe shall:

(1) Create and maintain an investigative report on each background investigation. An investigative report shall include all of the following:

(i) Steps taken in conducting a background investigation;

(ii) Results obtained;

(iii) Candidates matched; and

(iv) The basis for those conclusions.

(2) Submit a notice of results of the applicant's background investigation to the Commission no later than sixty (60) days after the applicant begins work. The notice of results shall contain:

(i) Applicant's name, date of birth, and social security number;

(ii) Date on which applicant began or will begin work as key employee or primary management official;

(iii) A summary of the information presented in the investigative report, which shall at a minimum include a listing of:

(A) Licenses that have previously been denied;

(B) Gaming licenses that have been revoked, even if subsequently reinstated;

(C) Every known criminal charge brought against the applicant within the last 10 years of the date of application; and

(D) Every felony of which the applicant has been convicted or any ongoing prosecution.

---

---

---

---

---


---

---

---

---

---



## How can CHRI impact Part 558.3?

A tribe shall retain the following for no less than three years from the termination.

- Investigative reports
- Eligibility determinations

**Regulations**

**Non-Indian Individual Offenses Under the U.S. Government Crime Statutes**

For questions on CHRI training classes, please see 1985-1986 and 1987-1988 (see 1985-1986 and 1987-1988) (see 1985-1986 and 1987-1988)

**558.3**

The application, having filed accurate the objectives referred to by the Commission, the tribe shall make the final decision whether to issue a license to such applicant.

(A) If the tribe has issued the license before receiving the Commission's statement of objections, notice and hearing shall be provided to the licensee as provided by 558.4A.

(7)(A) (2019, Jan. 21, 2019, as amended in 1997 (1997, Apr. 12, 2019))

**558.3 Notification to NIGC of license decisions and retention obligations.**

(A) When a tribe has provided a notice of results of the background check to the Commission, and the tribe may license a primary management official as key employee:

(i) Within 30 days after the issuance of the license, a tribe shall notify the Commission of its issuance.

(ii) A gaming operation shall not employ a key employee or primary management official who does not have a license after thirty (30) days.

(B) If a tribe does not license an applicant—

(1) The tribe shall notify the Commission; and

(2) Shall forward copies of its eligibility determination and notice of results, under 558.4(b)(2) of this chapter, to the Commission for inclusion in the Indian Gaming Individuals Record System.

(C) A tribe shall retain the following for inspection by the Chair or his or her designee for no less than three years from the date of termination of employment:

(i) Applications for licensing;

(ii) Investigative reports; and

(iii) Eligibility determinations.

**558.4**

---

---

---


---

---

---

---

---



## Contact Information:

[TrainingInfo@nigc.gov](mailto:TrainingInfo@nigc.gov)




---

---

---

---

---

---

---

---