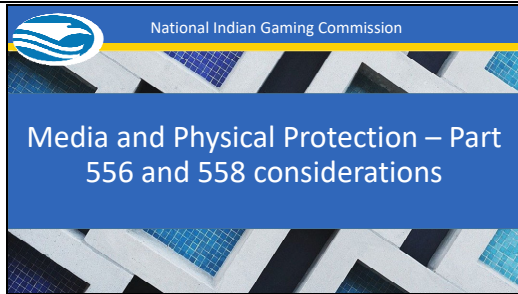


Slide 1



PARTICIPANT GUIDE

Chairman Simermeyer promotes four emphasis areas in the Agency’s work, and he is committed to being more engaged and accountable to the Indian gaming industry and Indian Country.

Industry Integrity

Protecting the valuable tool of Indian gaming that in many communities creates jobs, is the lifeblood for tribal programs, and creates opportunities for tribes to explore and strengthen relationships with neighboring jurisdictions.

Agency Accountability

Meeting the public’s expectation for administrative processes that uphold good governance practices and support efficient and effective decision making to protect tribal assets.

Preparedness

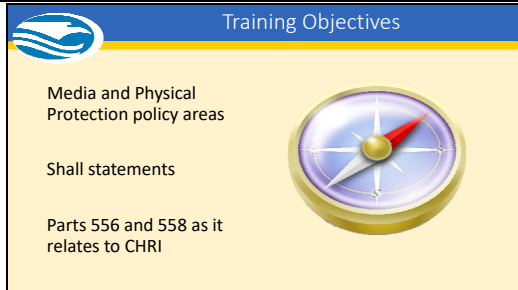
Promoting tribes’ capacity to plan for risks to tribal gaming assets including natural disaster threats, the need to modernize and enhance regulatory and gaming operation workforces, or public health and safety emergencies.

Outreach

Cultivating opportunities for outreach to ensure well-informed Indian gaming policy development through diverse relationships, accessible resources, and government-to-government consultation.

This training reinforces these four emphasis areas and the agency’s commitment to the Indian gaming industry and Indian Country.

Slide 2






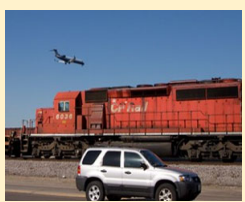
PARTICIPANT GUIDE






This training will review CJIS Security Policy Areas 5.8 (Media Protection) and 5.9 (Physical Protection), discuss the shall statements in the policy areas and provide guidance for compliance with Parts 556.4, 556.6 and 558.3, as it relates to CHRI.




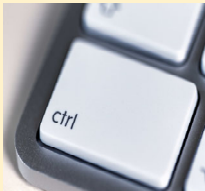

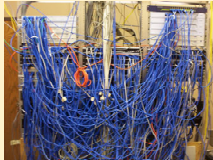






POLL QUESTION

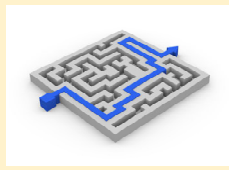
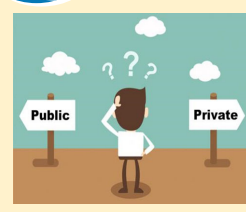

1. Are you a LASO?
 - a. Yes
 - b. No

2. Are you “authorized personnel?”
 - a. Yes
 - b. No

<p>Slide 3</p>	<p>What is CHRI?</p>  <p>Why the sad face?</p>	<p>PARTICIPANT GUIDE</p> <p>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. 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. 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.</p>
<p>Slide 4</p>	<p>5.8 Media Protection</p> <p>Procedures <u>shall</u> be documented and implemented.</p> <p>Procedures <u>shall</u> be defined for securely handling, transporting and storing media.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.8 Policy Area 8: Media Protection</p> <p>Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.</p>
<p>Slide 5</p>	<p>5.8.1 Media Storage and Access</p> <p><u>Shall</u> securely store digital and physical media</p> <p><u>Shall</u> restrict access</p> <p>If not, <u>shall</u> be encrypted per Section 5.10.1.2.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.8.1 Media Storage and Access</p> <p>The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.</p>
<p>Slide 6</p>	<p>5.8.2 Media Transport</p> <p><u>Shall</u> protect and control digital and physical media during transport outside of controlled areas.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.8.2 Media Transport</p> <p>The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.</p> <p>5.8.2.1 Digital Media during Transport</p> <p>Controls shall be in place to protect digital media containing CJJ while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.</p> <p>5.8.2.2 Physical Media in Transit</p> <p>The controls and security measures in this document also apply to CJJ in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.</p>


<p>Slide 7</p>	<p>5.8.3 Digital Media Sanitization/Disposal</p> <p><u>Shall</u> sanitize before disposal or release</p> <p><u>Shall</u> maintain written documentation</p> <p>Inoperable media <u>shall</u> be destroyed</p> <p><u>Shall</u> ensure the sanitization or destruction is witnessed or carried out by authorized personnel</p> 	<p>PARTICIPANT GUIDE</p> <p>5.8.3 Digital Media Sanitization and Disposal</p> <p>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.). 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.</p>
<p>Slide 8</p>	<p>5.8.4 Disposal of Physical Media</p> <p><u>Shall</u> be securely disposed of when no longer required, using formal procedures.</p> <p><u>Shall</u> be destroyed by shredding or incineration.</p> <p><u>Shall</u> ensure the disposal or destruction is witnessed or carried out by authorized personnel.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.8.4 Disposal of Physical Media</p> <p>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. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.</p>
<p>Slide 9</p>	<p>5.9 Physical Protection</p> <p>Physical protection policy and procedures <u>shall</u> be documented</p> 	<p>PARTICIPANT NOTES</p> <p>5.9 Policy Area 9: Physical Protection</p> <p>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.</p>
<p>Slide 10</p>	<p>5.9.1 Physical Secure Location</p>  <p>A room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems</p>	<p>PARTICIPANT NOTES</p> <p>5.9.1 Physically Secure Location</p> <p>A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof. Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.</p>
<p>Slide 11</p>	<p>5.9.1.1 Security Perimeter</p> <p><u>Shall</u> be prominently posted and separated from non-secure locations</p> <p><u>Shall</u> be defined, controlled and secured in a manner acceptable to the CSA</p> 	<p>PARTICIPANT GUIDE</p> <p>5.9.1.1 Security Perimeter</p> <p>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.</p>

<p>Slide 12</p>	<p> 5.9.1.2 Physical Access Authorizations</p> <p><u>Shall</u> develop and keep current an APL to the PSL...</p> <p>or <u>shall</u> issue credentials to authorized personnel.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.9.1.2 Physical Access Authorizations</p> <p>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.</p>
<p>Slide 13</p>	<p> 5.9.1.3 Physical Access Control</p>  <p><u>Shall</u> control all physical access points...</p> <p>and <u>shall</u> verify individual access authorizations before granting access.</p>	<p>PARTICIPANT GUIDE</p> <p>5.9.1.3 Physical Access Control</p> <p>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.</p>
<p>Slide 14</p>	<p> 5.9.1.4 Access Control</p> <p><u>Shall</u> control physical access to information system distribution and transmission lines within the physically secure location.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.9.1.4 Access Control for Transmission Medium</p> <p>The agency shall control physical access to information system distribution and transmission lines within the physically secure location.</p>
<p>Slide 15</p>	<p> 5.9.1.5 Access Control</p> <p><u>Shall</u> control physical access to information system devices that display CJJ</p> <p><u>Shall</u> prevent unauthorized individuals from accessing and viewing CJJ.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.9.1.5 Access Control for Display Medium</p> <p>The agency shall control physical access to information system devices that display CJJ and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJJ.</p>
<p>Slide 16</p>	<p> 5.9.1.6 Monitoring Physical Access</p>  <p><u>Shall</u> monitor physical access to the information system to detect and respond to physical security incidents.</p>	<p>PARTICIPANT GUIDE</p> <p>5.9.1.6 Monitoring Physical Access</p> <p>The agency shall monitor physical access to the information system to detect and respond to physical security incidents.</p>
<p>Slide 17</p>	<p> 5.9.1.7 Visitor Control</p> <p><u>Shall</u> control physical access by authenticating visitors</p> <p><u>Shall</u> escort visitors at all times and monitor visitor activity.</p> 	<p>PARTICIPANT GUIDE</p> <p>5.9.1.7 Visitor Control</p> <p>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.</p>

<p>Slide 18</p>	<p>5.9.1.8 Delivery and Removal</p>  <p>Shall authorize and control information system-related items entering and exiting the physically secure location.</p>	<p>PARTICIPANT GUIDE</p> <p>5.9.1.8 Delivery and Removal</p> <p>The agency shall authorize and control information system-related items entering and exiting the physically secure location.</p>
<p>Slide 19</p>	<p>5.9.2 Controlled Area</p>  <ul style="list-style-type: none"> • Limit access and lock the area when unattended • Position devices and documents to prevent access/view • Encrypt “at rest” 	<p>PARTICIPANT GUIDE</p> <p>5.9.2 Controlled Area</p> <p>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 CJJ, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJJ access or storage. The agency shall, at a minimum:</p> <ol style="list-style-type: none"> 1. Limit access to the controlled area during CJJ processing times to only those personnel authorized by the agency to access or view CJJ. 2. Lock the area, room, or storage container when unattended. 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.
<p>Slide 20</p>	<p>How can CHRI impact Part 556.6?</p>  <ul style="list-style-type: none"> • Every known criminal charge within the last 10 years. • Every felony conviction or any ongoing prosecution. 	<p>PARTICIPANT GUIDE</p> <p>§556.6 Report to the Commission.</p> <p>(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).</p> <p>(b) Before issuing a license to a primary management official or to a key employee, a tribe shall:</p> <ol style="list-style-type: none"> (1) Create and maintain an investigative report on each background investigation. An investigative report shall include all of the following: <ol style="list-style-type: none"> (i) Steps taken in conducting a background investigation; (ii) Results obtained; (iii) Conclusions reached; 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: <ol style="list-style-type: none"> (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: <ol style="list-style-type: none"> (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. <p>(iv) A copy of the eligibility determination made under §556.5.</p>


Slide 21

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




PARTICIPANT GUIDE

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


- (a) After a tribe has provided a notice of results of the background check to the Commission, a tribe may license a primary management official or key employee.
- (b) Within 30 days after the issuance of the license, a tribe shall notify the Commission of its issuance.
- (c) A gaming operation shall not employ a key employee or primary management official who does not have a license after ninety (90) days.
- (d) 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 §556.6(b)(2) of this chapter, to the Commission for inclusion in the Indian Gaming Individuals Record System.
- (e) 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:
 - (1) Applications for licensing;
 - (2) Investigative reports; and
 - (3) Eligibility determinations.

Slide 22

Thank you



Contact Information:
TrainingInfo@nigc.gov



INSTRUCTOR NOTES

If you have any questions about this training or if you are interested in a site-specific training on these topics, please email traininginfo@nigc.gov.

Thank you!