PUBLIC DEFENDER
ACCESS TO CJI FOR DISCOVERY
03/29/2021

GUIDE FOR HANDLING CRIMINAL JUSTICE INFORMATION

PURPOSE:

Assist contracting agencies and public defenders in clarifying the use of Criminal Justice Information (CJI) for the purpose of discovery.

CONCLUSION:

"The prosecution may share the CHRI of criminal defendants and witnesses with defense counsel if the information is already part of the prosecution's file and is subject to an ongoing discovery obligation. It is assumed that the CHRI is already in the possession of the prosecution as a result of appropriate access for its own use pursuant to the provisions of the CFR. As such, the CHRI is effectively part of the prosecution's own records and secondary dissemination pursuant to a court order is permissible.

In instances in which the prosecutor has not obtained CHRI for the defendant or witnesses, the Court may order the FBI to produce the CHRI for review by the court. The order should contain language that the FBI is to provide the requested criminal history record information to the court. If your rules require the redaction of the identifying biographic information, the unit will accept this information in a separate communication. The requested criminal history record information cannot be obtained without the identifying biographic information. A certified copy of the order should be sent to the following address:

FBI, CJIS Division
1000 Custer Hollow Road
Clarksburg, West Virginia 26306
Attn: Biometric Services Section, Criminal History Analysis Team 1

The FBI will provide the Court with the requested records. The records produced will be accompanied by a letter requesting the Court to review the CHRI prior to providing it to the respective parties to insure that it is relevant to the matter before the Court. For example, pursuant to most rules of evidence and procedure, a stale misdemeanor conviction could not be used to impeach a witness; hence, dissemination by the Court to defense counsel would not serve a proper function." (See full FBI response.)

Any sharing of CHRI must follow the guidelines and adhere to all laws and policies.

AUTHOR

Karla Mead
NCJIS Criminal Compliance Auditor/Business Process Analyst II
Department of Public Safety – Records, Communications and Compliance Division

POINT OF CONTACT

Questions regarding this topic should be directed to:

Criminal Compliance: NCJIS Compliance Audit staff at CriminalAuditor@dps.state.nv.us.

BACKGROUND AND FINDINGS

Criminal history queries, specifically those of the CJIS division's Interstate Identification Index (commonly referred to as "Triple I" or "III"), has several regulations, requirements, and responsibilities that accompany it.

Agencies must ensure that users perform queries for authorized purposes, use the correct purpose code, and maintain a log of why they are performing the query. Title 28 CFR Part 20 details the requirements placed upon the FBI, State CJIS System Agency (CSA), and local agencies as it relates to federal computerized criminal history (CCH).

There has been confusion amongst criminal justice agencies on what they can and cannot disseminate to public defenders. Agencies with an FBI issued ORI have a User Agreement to access the State system. Several agencies have refused to share information with public defenders, and other agencies have allowed it for the purpose of discovery.

Some public defenders have provided copies of Criminal History Record Information (CHRI) to their clients. There have been several cases where CHRI has been transferred through jail facilities and confiscated. These incidences have been reported to audit staff for resolution.

It is required to stamp CHRI disseminated for the purpose of discovery with "Confidential, do not further disseminate". Courts have been directed to educate entities on proper CHRI practices. It has also been recommended during audit that agencies have public defenders sign an acknowledgement or a Declaration of Understanding (DOU) upon release to help ensure no mishandling or misuse.

While dissemination of CHRI obtained by fingerprint submission to the applicant is permitted, CHRI obtained through a biographic submission is not authorized for dissemination directly to the applicant. These inquiries through JLINK are name based and not fingerprint based, therefore not guaranteed to be the subject of record. The risk of disseminating another's personal identifiers is probable and could open agencies and the State of Nevada to potential liability.

TECHNICAL OVERVIEW:

Agencies have been found emailing CHRI or placing CHRI into shared drive systems that provide access to unknown personnel. This is considered gross misuse that can result in severe penalties. The emailing of CHRI requires authorization from the Department of Public Safety Information Security Officer (ISO). The ISO will ensure that all requirements are met prior to granting authorization and will follow-up to ensure technical physical security. The FBI has strict criteria that must be met to email CHRI.

There are numerous ways to transmit Criminal Justice Information (CJI) electronically. Some methods can be relatively inexpensive whereas other methods can have a large financial investment to achieve.

DPS recommends using a traditional fax that uses plain analog phone lines to transmit CJI data across different secure locations. The receiving fax machine should be located in a physically secured area so that document is not sitting unattended for a non-authorized person to retrieve.

DPS recommends using a traditional fax to transmit CJI data. CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in CJIS Security Policy Section 5.10.

REFERENCE POLICY

State Policy

"CJI shall be used solely for the purpose for which it was requested and shall not be reproduced for secondary dissemination to any unauthorized entity, agency or person. User Agency must also agree and understands that if it disseminates any CJI to an unauthorized entity, agency or person, the User Agency and/or Authorized User may be subject to civil and criminal penalties under NRS 179A." **NCJIS Administrative Policy, 5.4, Dissemination, Secondary Dissemination #7**

"It is considered best practice to have Public Defenders and Attorneys sign a Declaration of Understanding governing Federal and State Dissemination and Confidentiality Laws as outlined in Title 28, Part 20, Code of Federal Regulations and NRS 179A." **NCJIS Administrative Policy, 5.4, Dissemination, Secondary Dissemination Note**

"All information from the FBI's Interstate Identification Index (III) must be redacted from any report prior to dissemination to an unauthorized source. This includes public release to media." **NCJIS Administrative Policy, 5.4, Dissemination, Secondary Dissemination #4**

"Any transactions pulled from NCJIS/FBI CJIS systems are name-based reports and should not be disseminated to inmates or other possible subjects of record. Any subject that wishes to obtain

a copy of their Nevada record of criminal history should contact the Department of Public Safety, Records, Communications and Compliance Division to request their fingerprint-based results. Requests for FBI records of criminal history for personal use should be directed to the FBI. **NCJIS Administrative Policy, 5.4, Dissemination, Secondary Dissemination #5**
"All III extracted from the state message switch is governed by both federal and state law which must be considered when hardcopy and verbal information is disseminated." **NCJIS Administrative Policy, 5.4, Dissemination, Secondary Dissemination #6**

"TACs must establish IWPs specific to their agency regarding dissemination of CHRI. A current list of the agency's authorized personnel must be referenced in the IWP and made available to the agency's available to the agency's terminal operators. Disseminating CHRI from any system of NCJIS or FBI CJIS System to any unauthorized person or agency is prohibited." **NCJIS Administrative Policy, Dissemination**

"Agencies are not allowed to email CJI even if the email is encrypted without the express written permission from the CSO or designee. Exceptions will be permitted in exceptional situations that require business continuity for the requesting agency or in other exceptional situations i.e., natural disaster, human life at risk, etc. Each individual request will be reviewed at the discretion of the CSO or designee." **Nevada Administrative Policy, Section 3 Technical, 3.5 Logical Security #4**

"If an agency plans to move CJI across any wireless technology, please contact the Nevada CJIS ISO for prior configuration consultation." **NCJIS Administrative Policy, Section 3 Technical Security, 3.5 Logical Security #6**

Penalty if Not Enforced:

"CJI must be used for the purpose for which it was provided and afforded the maximum protection. It is forbidden for agency personnel to request and/or perform inquiries for curiosity. Any inquiry other than a criminal justice purpose must be governed by a federal, state or local statute(s)." **NCJIS Administrative Policy, 5.4, Criminal Justice Information, Section 5.1 #4**
Federal Policy

"Authorized agencies must not use the III for remotely accessing a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing to either the FBI's CJIS Division or the state of record accompanied by fingerprints." **NCIC III/NF Manual 1.1.4 Prohibited Use**

"Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for

criminal justice employment applicants." **CJIS Security Policy 4.2.1 Proper Access, Use, and Dissemination of CHRI**

"Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties." **4.2.5.2 Penalties**

"The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know." **CJIS Security Policy 5.5.2.1 Least Privilege**

"Authorized agencies must not use the III for remotely accessing a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing to either the FBI's CJIS Division or the state of record accompanied by fingerprints." **NCIC III File - 1.1.4 Prohibited Use**

"CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting, and storing media. "Electronic media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g., printed documents, printed imagery, etc." **CJIS Policy 5.8 – Media Protection**

"CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per **CSP Section 5.10.1.2.**"

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.

"CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the

encryption requirements for CJI in transit as defined in Section 5.10." **CJIS Security Policy 5.10.2**

"When CJI is at rest (i.e., stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 of the CJIS policy or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength." **CJIS Security Policy 5.10.1.2.2**

"When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI.: **CJIS Security Policy 5.10.1.2.1**

Penalty if Not Enforced:

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties. **CJIS Security Policy 4.2.5.2 Penalties**

FBI RESPONSE TO PUBLIC DEFENDERS AND DISSIMINATION

In circumstances where criminal history record information (CHRI) has not been previously obtained by the prosecution for its own use, access to the NCIC/III by the prosecution to obtain CHRI about the defendant or witnesses (including victims) solely on behalf of defense counsel should not occur. To allow otherwise would effectively authorize the production of FBI-maintained records by a local prosecutor. In instances in which the prosecutor has not previously obtained the CHRI and is directed by the judiciary to provide such information, we have admonished prosecutors that court orders of this nature should be resisted and referred to this office for handling in accordance with federal laws and regulation. Failure to do so may result in termination of NCIC access.

Dissemination of CHRI by the FBI is governed by 28 USC 534 and federal regulations found in 28 CFR Part 20. These authorities essentially restrict dissemination of CHRI to "criminal justice agencies for criminal justice purposes." Dissemination of FBI CHRI is also governed by the Freedom of Information Act (5 USC 552) and the Privacy Act of 1974 (7 USC 552a).

Pursuant to 28 USC 534, the FBI is responsible for acquiring, collecting, and preserving identification, criminal identification, crime, and other records. The FBI is also responsible for exchanging such records with, and for the official use of the federal government, the states, cities, and penal and other institutions. Rules governing access to and dissemination of FBI CHRI obtainable through NCIC are set forth in 28 CFR Part 20. The term "criminal justice agency" is defined at 28 CFR 20.3(g) as "(1) Courts; and (2) A governmental agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration

of criminal justice." The "administration of criminal justice" is defined as "the performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders." These terms must be read together. NCIC terminal access is predicated upon a criminal justice agency engaging in an administration of criminal justice function. Failure to satisfy either of these prongs will result in a denial of authorized access to NCIC/III records.

Criminal defense attorneys do not have direct access to FBI-maintained CHRI for criminal defense purposes. The definitions of "criminal justice agency" and "administration of criminal justice" found in 28 CFR 20.3 do not include criminal defense functions, whether performed by a public defender or retained or appointed counsel.

The restrictions on direct access can be accommodated by an order of a court of competent jurisdiction. Courts have inherent and/or statutory powers to procure relevant evidence and ensure fairness in proceedings. Federal law and policy recognize the existence of such powers and, in most cases, accommodate the exercise of such powers with respect to dissemination of CHRI pertaining to defendants and witnesses.

The prosecution may share the CHRI of criminal defendants and witnesses with defense counsel if the information is already part of the prosecution's file and is subject to an ongoing discovery obligation. It is assumed that the CHRI is already in the possession of the prosecution as a result of appropriate access for its own use pursuant to the provisions of the CFR. As such, the CHRI is effectively part of the prosecution's own records and secondary dissemination pursuant to a court order is permissible.

In instances in which the prosecutor has not obtained CHRI for the defendant or witnesses, the Court may order the FBI to produce the CHRI for review by the court. The order should contain language that the FBI is to provide the requested criminal history record information to the court. If your rules require the redaction of the identifying biographic information, the unit will accept this information in a separate communication. The requested criminal history record information cannot be obtained without the identifying biographic information. A certified copy of the order should be sent to the following address:

FBI, CJIS Division
1000 Custer Hollow Road
Clarksburg, West Virginia 26306
Attn: Biometric Services Section, Criminal History Analysis Team 1

The FBI will provide the Court with the requested records. The records produced will be accompanied by a letter requesting the Court to review the CHRI prior to providing it to the respective parties to insure that it is relevant to the matter before the Court. For example, pursuant to most rules of evidence and procedure, a stale misdemeanor conviction could not be used to impeach a witness; hence, dissemination by the Court to defense counsel would not serve a proper function.

I hope this information helps. If you need any additional information, please do not hesitate to contact me. Also, please feel free to pass this information along to any parties impacted by this issue. I am happy to answer any questions that they may have.

CJIS Division
Biometric Services Section

RECCONMENDATIONS TO ENSURE NO MISUSE

The Department of Public Safety has the below recommendations to ensure the proper use and protection of criminal justice and Criminal History Record Information (CHRI).

Contracted Authorized Agencies

- Stamp all secondary dissemination as Confidential -not for further dissemination."
- Log secondary dissemination as defined in Nevada Administrative Policy and CJIS Security Policy.
- Do not disseminate any information from JLINK that is not for the purpose of discovery. (Only share information if it is already a part of the prosecutions file.)
- Do not run and provide CHRI to any unauthorized sources or without proper authority.
- Do ensure that anyone receiving information for the purpose of discovery is versed on the laws governing the protection of such data.
- If you choose to use a share drive, contact the State ISO team for review and approval.
- Do fax, mail, or signature pickup up (authorized personnel) to securely transport CJI/CHRI.
- Do not email CHRI. In-order-to email CHRI you must have specific measures in place, and this requires approval from the DPS ISO. (Reference CJIS Security Policy for further clarification.)
- Encourage the use of CJIS Online for training purposes.

Public Defenders

- Do not pass information to your clients. These records are name-based and not a guarantee of the subject of record.
- Do not pass/transfer information through jail facilities.
- Make sure received information is stamped "Confidential"
- Do refer your client to the Department of Public Safety – Central Repository if they wish to have a copy of their fingerprint-based background check/criminal history.
- Encourage training of all staff on the handling of CJI. (See state training recommendations.)
- Track chain of custody.
- Destroy by shred or burn only when no longer needed. (Disposal by other means is not permitted.)
- Secure all electronic means of storage or transfer of CJI/ CHRI. This requires ISO approval.

- Be familiar with NRS, CFR and USC governing CJI.
- If you wish to obtain CHRI/CJI for the defendant or witness, you may have a court order issued and submitted to the FBI to produce such records. (See FBI response for further).
- Do not allow unauthorized staff, contractors, or unauthorized personnel to view, hear or handle CJI/CHRI. We recommend that janitorial staff and contractors be escorted around CJI/CHRI data. Unescorted access requirements are defined in CJIS and Nevada Administrative Policy.

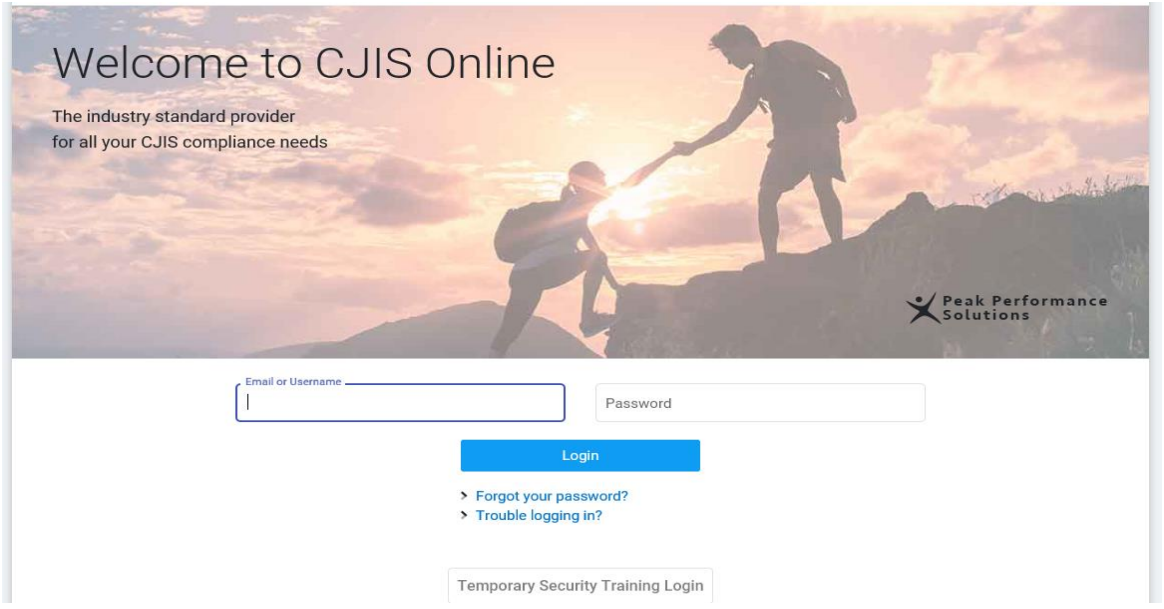
TRAINING

CJIS Online

CJIS Online is CJIS Security Awareness Training that provides Nevada agencies and entities with the proper training outlined in CJIS Security Policy 5.2. This is a web-based training offered by the State of Nevada at no cost to assist agencies in meeting training requirements. It can be used in conjunction with your agencies Internal Written Policies and Procedures to ensure the protection of CJI/CHRI.

It is recommended that all agencies that see, hear or touch CJI complete Level 2 CJIS Online training. Level 2 – Physical access to CJI/CHRI obtained within the Nevada Criminal Justice Information System.

It is recommended that all IT support staff or personnel that have unescorted access to routers, switches, servers that process, store, or transmit CJI complete Level 4 CJIS Online training. This includes the securing of such equipment. Level 4 – Personnel with information technology roles.



https://www.cjisonline.com/

For further information regarding CJIS Security Awareness Training with CJIS Online, please contact: CriminalAuditor@dps.state.nv.us.

Declaration of Understanding

Contracted Agencies

A Declaration of Understanding (DOU) is primarily in place to assist agencies in reducing liability. It is required by Nevada Administrative Policy and signed User Agreements that all employees sign a DOU. These documents must be kept on file and available for review by audit staff upon request.

Public Defenders

Any non-contracted public defenders' entity that is viewing, discussing, receiving, or handling criminal justice information for the purpose of discovery. should consider the use of a DOU to assist in limiting misuse and mishandling of information obtained from the Nevada Criminal Justice Information System.

The below template can be personalized to fit your agencies specific practices.

Declaration of Understanding

Criminal Justice Information

_____ *(Employee name)* _____, as an employee of _____ (*Agency name)* _____, in connection with my official duties, have access to confidential Criminal Justice Information (CJI).

1. Failure to follow these procedures shall result in the following disciplinary procedures:
    - First failure *(enter consequence)*
    - Second failure *(enter consequence)*
    - Third failure *(enter consequence)*
2. CJI must always be protected from unauthorized access.
3. All CJI is confidential and may not be discussed outside the working environment.
4. I acknowledge that CJI/CHRI extracted from Justice Link (JLINK) is name based and not a guarantee of the subject of record.
5. CJI will only be disseminated to authorized personnel as prescribed by law.
6. All CJI will be stored in the locked file cabinet as prescribed by TAC/Agency Administrator.
7. CJI will be shredded/burned only by an authorized person, when no longer needed.
8. CHRI will only be used for the purpose of discovery as outlined.

I have read and understand the above regulations regarding the use of CJI records

_____ _____

Signature Date