CJIS - NCJ Policy Manual

A Guide For Fingerprint-Based Access Of Criminal History Record Information Used For Non-Criminal Justice Purposes

VERSION 1.3
08/01/2023

Department of Public Safety
MISSOURI STATE HIGHWAY PATROL
Colonel Eric T. Olson, Superintendent

An Internationally Accredited Agency

Michael L. Parson
Governor

Sandra K. Karsten
Director

February 1, 2023

To: All Agencies with Access to Fingerprint-Based Criminal History Information for Noncriminal Justice Purposes

This manual, which is a supplement to the FBI CJIS Security Policy, reflects changes in policy, technology, and law as they occur. It also will provide each user a dependable, reliable, and easily accessible reference.

Realizing the multiple tasks all of you endure, I would encourage each of you to take the time necessary to become familiar with this manual. It is our hope this document will assist in forming stronger partnerships and promote better compliance with state and federal rules and regulations that govern access. Given the recent and justified scrutiny surrounding this type of information, we hope you will agree these goals are essential to keeping criminal history information available to those who have demonstrated a legitimate need.

As a user of fingerprint-based criminal history, this manual may be incorporated into your own agency policy and procedures for reference. Whether you use the criminal history for employment, licensing, permits, or for some other authorized benefit, this manual will serve to clarify the responsibilities each of us have and will help ensure criminal history information is protected and used according to law.

The Patrol's CJIS Division is dedicated to providing quality and professional service to our user community, and we look forward to assisting you in any way possible. Included in the manual is a list of contacts available should questions or problems arise.

Sincerely,

Gara N. Howard

GARA N. HOWARD, Captain
Criminal Justice Information Services Division

CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
Mailing Address: P.O. Box 9500, Jefferson City, MO 65102-9500
Street Address: 1510 East Elm Street, Jefferson City, MO 65101
Telephone: 573-526-6153 • FAX: 978-244-5247 • V/TDD: 573-751-3313
www.statepatrol.dps.missouri.gov

Table of Contents

SECTION 5: Security Awareness Training

SECTION 6: Policy Compliance Reviews (Pcr) / Audits

SECTION 7: Security & Management Control Outsourcing Standard

SECTION 8: Fingerprint Submission

SECTION 9: Criminal History

SECTION 10: State Agency, Board, Or Commission

SECTION 11: Missouri Vechs Program

SECTION 1: Introduction

1.1 Mission Statement

The Missouri State Highway Patrol will serve and protect all people by enforcing laws and providing services to ensure a safe and secure environment.

1.2 The Purpose Of This Manual

The purpose of this manual is to provide noncriminal justice agency (NCJA) users with clearly defined guidelines pertaining to use, retention, security, destruction, and dissemination of fingerprint-based criminal history record information (CHRI). It is intended to serve as an easy-to-use source of information, and to provide answers to questions that surface during everyday use of CHRI.

In order for all agencies with access to CHRI to operate within the high standards required, all users must have a good understanding of what is expected of them and comply at all times with established rules and regulations.

The policies and procedures in this manual apply to every individual, contractor, private entity, NCJA representative, or member of a criminal justice entity, with access to fingerprint-based CHRI derived from the systems of the Missouri State Highway Patrol Criminal Justice Information Services Division (MSHP-CJISD) and U.S. Department of Justice, Federal Bureau of Investigation (FBI). This manual serves as a supplement to the FBI CJIS Security Policy.

1.3 The MSHP-CJISD Is The Central Repository

All collection and dissemination of CHRI is in compliance with Chapter 610 RSMo, Chapter 43 RSMo, and applicable federal laws or regulations. The MSHP-CJISD is responsible for compiling and disseminating complete and accurate criminal history records and for the compiling, maintaining, and dissemination of criminal incident and arrest reports and statistics. CHRI is collected by criminal justice agencies on individuals which consists of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising from sentencing, correctional supervision, and release.

Although the primary function of the Central Repository is the administration of criminal justice, the record information retained is available for noncriminal justice purposes. Laws governing the dissemination of open and closed record information are regulated by state statute. (Section 610.120 RSMo, and Title 11 Code of State Regulations (CSR) Division 30, Chapter 4.)

1.4 A Policy Is A Guideline

Guidelines are based on a law or the decisions of a rulemaking authority. Policies help the user understand what may or may not be done with the fingerprint-based CHRI. This manual also dictates sanctions for policy violations.

1.5 A Procedure Is A Method

A procedure is a process or series of steps taken to accomplish a task. Procedures are methods and they are ways of carrying out a policy. The procedures in this manual may dictate actions that must be taken, when and how tasks are achieved, or who takes steps and why they are taken. Procedures also incorporate forms which are referenced and accessible through the MSHP's website.

SECTION 2: Authority

2.1 How Policy Is Formulated

The FBI has designated the MSHP-CJISD as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Missouri. The superintendent of the MSHP appoints a CJIS Systems Officer (CSO) for the state. The CSO is responsible for ensuring that all agencies with access to CHRI adhere to state and federal laws.

The MSHP has been the Central Repository for fingerprint and criminal arrest information since 1934, when the Bureau of Identification was established within the MSHP. The bureau was not officially designated in state statute until 1986, when the 83rd General Assembly of the state of Missouri passed House Bills 873 and 874. These bills were introduced and overwhelmingly passed based on the premise of the need to protect victims of violent crimes and the need to provide a greater voice to those impacted by crime. On May 12, 1986, legislation was signed and the bills became law in August that same year. Chapter 43 of the Missouri Revised Statutes formally designated the Bureau of Identification as the Central Repository of Missouri. As a result of the passing of these bills, the Missouri State Highway Patrol's Bureau of Identification was designated as the Central Repository for compiling, storing, and disseminating CHRI. The bill further required the mandatory reporting of all felony and serious or aggravated misdemeanor criminal arrest information by law enforcement personnel, prosecuting attorneys, courts, Department of Corrections, and the Department of Mental Health. The Central Repository is the sole source communicator of Missouri criminal history records to the FBI. In 1991, the Bureau of Identification was renamed to the Criminal Records and Identification Division, and again renamed in 2009, to the Criminal Justice Information Services (CJIS) Division. The CJIS Division functions under the Technical Services Bureau.

The term "non-criminal justice purposes" is defined by the National Crime Prevention and Privacy Compact Council as uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

2.1.1 The CJIS Advisory Policy Board (APB) establishes policy concerning the philosophy, concept, and operational principals of the National Crime Information Center (NCIC). It reviews policy, and technical and operational issues in order to make recommendations to the director of the Federal Bureau of Investigation (FBI). The APB is comprised of 33 administrators from local, state, and federal criminal justice agencies throughout the United States and meets at least twice each calendar year.

2.1.2 The National Crime Prevention and Privacy Compact Council (Title 42, USC 14611-16), also referred to as "Compact" was signed into law on October 9, 1998, by President William Jefferson Clinton, allowing party states to disseminate their CHRI to other states for noncriminal justice purposes in accordance with the laws of the receiving state. The Compact was necessary to facilitate record sharing as it supersedes any conflicting laws in states where it is adopted and provides a uniform dissemination standard among states. The Compact provides for the establishment of a Council that shall have the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. The Compact is composed of 15 members appointed by the U.S. attorney general. The membership composition and terms specified under Article VI of the Compact requires nine of the 15 Council members to be state compact officers or state repository administrators.

2.1.3 The National Crime Information Center (NCIC) is maintained by the FBI's CJIS Division. The purpose of NCIC, according to the FBI, is: "to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending fugitives, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system."

2.1.4 The Interstate Identification Index (III) is a "cooperative federal-state program for the interstate exchange of CHRI for the purposes of facilitating the interstate exchange of such information among criminal justice agencies." This database was initially created for the use of government agencies involved in the administration of criminal justice functions; however, over time, the use of this information has been authorized for numerous noncriminal justice purposes, such as background screening for employment and licensing. The III system is quite comprehensive in its coverage of nationwide arrest records for serious offenses.

2.1.5 The Missouri Uniform Law Enforcement System (MULES) is Missouri's law enforcement computer network. The MULES network was implemented in 1969, within the Information Systems Division (ISD), presently the CJIS Division of the MSHP. MULES originated as a computerized information system to serve all criminal justice agencies in Missouri.

2.1.6 The Automated Fingerprint Identification System (AFIS) is a computer system that interfaces with the criminal history component of MULES and electronically images and stores the characteristics of fingerprint patterns. Fingerprint identification has been a major responsibility of the MSHP since 1934, and the FBI since 1924. The CJIS Division within the FBI is the largest division and is responsible for administering several programs including the Integrated Automated Fingerprint Identification System (IAFIS); the NCIC including the III and other files of interest to law enforcement, such as those relating to wanted persons, civil protection orders, registered sex offenders, and missing persons; and the National Instant Criminal Background Check System (NICS) which processes background checks on prospective purchasers of firearms from federal firearm licensees. (Attorney General Report on Criminal History Background Checks, June 2006.)

2.1.7 CJIS Security Policy — The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI), whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. This policy applies to every individual, including contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity, with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including in those states with separate authorities, the SIBs. Further, as use of CHRI for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the Compact and state compact officers in the secure exchange of criminal justice records.

The CJIS Security Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The policy empowers CSAs with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the board spectrum of the criminal justice and noncriminal justice communities.

For viewing and/or download of the CJIS Security Policy, please click:

https://apps.mshp.dps.mo.gov/MSHPWeb/DevelopersPages/CRID/handbooksAndManuals.html#CJIS

2.1.8 Revised Statutes of Missouri (RSMo) — The MSHP operates and administers the Missouri Uniform Law Enforcement System (MULES) in accordance with the Revised Statutes of Missouri, Chapter 43, section 43.509 RSMo, designates the MSHP as the Central Repository for CHRI.

SECTION 3: AGENCY ACCESS

3.1 ORI Assignment

An Originating Agency Identifier (ORI) is a nine-character identifier, assigned by the FBI, and is used to identify authorized agencies and control access to the systems. To qualify for an ORI assignment for noncriminal justice purposes, an agency must be authorized under Public Law 92-544 with an approved state statute or authorized through federal legislation.

Each active ORI must have on file, with the MSHP-CJISD, two documents:

1. User Agreement (SHP-575 or SHP-982);
2. Local Agency Security Officer (LASO) form (SHP-988).

Every agency is responsible for ensuring documents are kept current and submit new forms should agency information change.

The LASO form is available in the documents section of an agency's MACHS portal account. The user agreement and LASO form may be obtained by contacting the regional CJIS Trainer/Auditor. Contact information is available in Appendix A of this document.

3.2 New Agency Application

Requests for access to criminal history must be made to the MSHP-CJISD. A letter of request, along with supporting legislative authority is required. The letter of request should state the purpose for the request and use of criminal history.

3.3 Public Law 92-544 Requirements

Prior to 1971, the FBI exchanged records with federal, state and local agencies for both criminal and noncriminal justice use; however, this practice was altered by Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971), in which the district court determined that "Congress never intended to or in fact did authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks." In response to Menard, the FBI immediately curtailed receipt of fingerprints for nonfederal licensing and employment screening.

Congress responded in December 1971 by enacting Public Law 92-184, 85 Stat. 627, 642 (1971) , which authorized the exchange of FBI identification records with officials of federally chartered or insured banking institutions to maintain the security of those institutions, and, if authorized by state statute approved by the Attorney General, to officials of state and local governments for purposes of employment and licensing. This statute was superseded in 1972 by Public Law 92-544, 86 Stat. 1115 (1972), which states: The funds provided for Salaries and Expenses, Federal Bureau of Investigation, may be used hereafter, in addition to those uses authorized thereunder, for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions, and, if authorized by State statute and approved by the Attorney General, to officials of State and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of any such official and subject to the same restriction with respect to dissemination as that provided for under the aforementioned appropriate.

The authority for the FBI to conduct a criminal record check for a noncriminal justice licensing or employment purposes is based upon Public Law 92-544. With this legislation, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the attorney general of the United States. The attorney general's authority to approve the statute is delegated to the FBI by Title 28, CFR Section 0.85(j). The standards employed by the FBI in approving Public Law 92-544 authorizations have been established by a series of memoranda issues by the Office of Legal Counsel, Department of Justice. The criteria are as follows:

a) The statute must exist as a result of a legislative enactment;

b) It must require the fingerprinting of applicants who are to be subjected to a national criminal history background check;

c) It must, expressly ("submit to the FBI") or by implication ("submit for a national check"), authorize the use of FBI records for the screening of applicants;

d) It must identify the specific category(ies) of licensees/employees falling within its purview, thereby avoiding overbreadth;

e) It must not be against public policy; and

f) It may not authorize receipt of the CHRI by a private entity.

Additionally, FBI policy requires that fingerprints be initially submitted to the state identification bureau (for a check of state records) and thereafter forwarded to the FBI for a "national" criminal history check.

Fingerprint card submissions to the FBI under Public Law 92-544 must be forwarded through the SIB. The state must also designate an authorized governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment or licensing. (Appendix B Criminal Justice Information Services (CJIS) Information Letter 95-3, Guidelines for implementing the NCPA/VCA Public Laws 103-209, 103-322).

3.4 ORI Structure

Every assigned ORI is unique to that agency. In Missouri, all ORI's will begin with letters "MO" and will be followed by seven characters. A noncriminal justice agency ORI will contain the letter "Z" in the ninth digit. The letter "Z" is used specifically to identify agencies receiving CHRI for noncriminal justice purposes, i.e., employment or licensing or other authorized benefit, according to state statute or federal law. Missouri Public Housing Authorities (PHAs), ORI's will contain the letter "Q" in the ninth digit.

3.5 Proper ORI Usage

ORIs are assigned by the FBI. All requests must be supported by statutory authority which meets Public Law 92-544 criteria. The statute must indicate fingerprint submission to the MSHP and FBI, listing the category of persons, and purpose for requesting criminal history.

3.6 Applicant Privacy Rights

During the May 2012 National Crime Prevention and Privacy Compact Council meeting, the Compact Council vetted the "Guiding Principles" for advising agencies receiving federally maintained CHRI of their obligation to notify applicants of their privacy rights in accordance with Title 28 CFR 50.12 regarding the exchange of FBI identification records. Records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments,

related agencies, or other authorized entities. Officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI.

The officials making the determination of suitability for licensing or employment shall provide the applicant the opportunity to complete or challenge the accuracy of the information contained in the FBI identification record.

These officials also must advise the applicant that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28 CFR 16.30-34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.

This policy is intended to ensure that all relevant criminal record information is made available to provide for the public's safety and, further, to protect the interests of the prospective employee or licensee who may be affected by the information, or lack of information in an identification record. (Order No. 2258-99, 64 FR 52229, September 29, 1999.)

The most current version of the Noncriminal Justice Applicant Privacy Rights and Privacy Statement may be found in forms, on the MSHP-CJISD website at the following link:
https://apps.mshp.dps.mo.gov/MSHPWeb/DevelopersPages/CRID/forms.html#CJIS

3.7 The Missouri and National Rap Back Program

With the passage of Section 43.540 RSMo, Missouri became the third participating state in the National Rap Back program through the Next Generation Identification (NGI) system. In Missouri, authorized agencies have the option of participation in the State Rap Back program or both the State and National Rap Back programs.

The purpose of the Rap Back programs is to provide updated Missouri and National fingerprint-based criminal arrest information on individuals who are employed with or who are otherwise under the purview of the authorized agency. The programs have a validation procedure requiring agencies to validate subscriptions on each enrolled applicant after three years from the date of fingerprint submission.

3.7.1 Rap Back Notification — Requires a criminal arrest where fingerprints are obtained. The notification process will be activated when a retained criminal ten-print fingerprint identification matches against an individual's subscription in Rap Back. The Rap Back subscription on an individual will remain until the individual is unenrolled by the agency holding the subscription. All Rap Back notifications are sent to agency Missouri Automated Criminal History System (MACHS) accounts via emails on file in the agency user account. MACHS users must log-in to their MACHS account to view the notification and request or opt-out for the individual. Notifications are available for 30 days. Failure to respond to a Rap Back notification within 30 days will trigger the permanent removal of each individual subscription awaiting a response. Re-activation of a Rap Back subscription requires the resubmission of fingerprints. Each agency is responsible for ensuring their Rap Back subscriptions are kept up-to-date and any subscriptions held where the individual is no longer employed or no longer under the agency's purview, must be removed. To ensure Rap Back subscriptions are kept current, the programs include a validation process.

3.7.2 Rap Back Validation — Refers to the process whereby the subscriber/agency holding the subscription, reviews an individual's subscription to determine whether they are still authorized to receive updates. Completing validations is a triennial process. If not properly validated, the Rap Back subscription will expire and the continuous services of receiving Rap Back notifications will be lost.

When a subscription requires validation, each agency MACHS user will receive an email advising of the validation requirement. The agency MACHS administrator must complete the validation process prior to the expiration date. Failure to complete the validations within 30 days will trigger the permanent removal of each individual subscription awaiting validation from Rap Back.

3.8 MACHS-II Portal Access for Electronic Results to CHRI

MACHS allows individuals within Missouri to register prior to being fingerprinted. For fingerprinting services, the State of Missouri contracts with a fingerprint vendor to capture fingerprint images and transmit those images, along with personally identifiable information (PII) to the MSHP-CJISD for processing.

Qualified entities eligible to receive Missouri closed records and FBI records, are provided a registration number to give to their applicants. The use of this number ensures the correct type of background check is conducted while at the same time ensuring the completed response is returned to the correct agency in a timely manner.

3.8.1 MACHS User Access - Agencies have the ability to request access to the Patrol's MACHS portal. User access is reviewed and approved through the MSHP-CJISD Information Security Unit. For new agency access, the use of a MACHS User Access form, SHP-383, is required.

The MACHS User Access Form requires the following fields:

- ORI
- OCA (if applicable)
- First Name, Middle Initial, Last Name of User
- Date of Birth (yyyy-mm-dd) of User
- Telephone Number and Extension of User, if applicable
- Last 4 digits of the Social Security Number of User
- Email Address of User (work email, not personal email)

In the "NEW User" field, check appropriate box. Options are:

- YES - New user
- NO - if request is for a modification to an existing user's account information

In the "Form Function" field, options are:

- Addition - for a new user
- Deletion - removing an existing user
- Modification - making a change to an existing user's account information
- If "Modification" is checked, enter explanation for change in the "Modifications" area.

In the "Access Level" (Check one) field, options are:

- ORI Administrator - the SHP-383 form is required
- ORI Read Only
- OCA Administrator
- OCA Read Only

Explanations of access levels are:

- **ORI Administrator Level** - this level is full access to add new users, delete existing users or make modifications to existing users for the agency. This level is responsible for Rap Back Validations and Rap Back Hit Notifications, if the agency participates in the Rap Back programs. The LASO of the agency must have administrator level access. Agencies may have more than one administrator.
- **ORI Read Only Level** - this level of access is assigned by the agency ORI Administrator/ LASO. The SHP-383 MACHS User Access Form is not required when the user information is being submitted by the agency administrator. This level of access can view, print and download criminal history responses. A user with this level does not have access to act on Rap Back validations or request Rap Back hit notifications.
- **OCA Administrator Level** - For agencies assigned an ORI and use OCAs (a sub-set of the ORI) with their ORI, the ORI Administrator for the agency can add users to this level of MACHS access or the MSHP CJIS Division can submit the request with the receipt of a completed SHP-383 form. For agencies enrolled in the Missouri VECHS Program, the MSHP CJIS Division must submit user access. VECHS agency users requesting OCA Administrator level must complete and submit an SHP-383 form. OCA Administrator level includes full access to add, modify, or delete users within the OCA Administrator designation. This level also has access to Rap Back Validations and Rap Back Hit Notifications.
- **OCA Read Only Level** - this level of access can be assigned by either the ORI or OCA administrator for the agency. This level of access can view, print and download the criminal history, but does not have access to act on Rap Back Validations or Rap Back Hit Notifications.

Examples of MACHS User Access Levels:

Missouri VECHS Program Entities - MACHS access levels include:

- OCA administrator level or OCA Read Only level
- For OCA Administrator access level, the user must complete the SHP-383 form. OCA Administrators can add users with OCA Read Only access.

State Agencies, City/County Municipalities - MACHS access levels include:

- ORI Administrator and ORI Read Only.
- For ORI Administrator level access, the SHP-383 form is required.

If the ORI assigned to the agency contains sub-set OCAs, the access levels will include options for OCA administrator and OCA Read only. In this instance, once the ORI Administrator is established, the administrator can add users for ORI Read Only, OCA Administrator and OCA Read Only. An OCA Administrator has the ability to add user access for OCA Read Only level.

Missouri public/charter school districts - MACHS access levels include:

- ORI Administrator and ORI Read Only
- Once an ORI Administrator is assigned, the administrator can add ORI Read Only users. If an additional ORI Administrator is required, the school district must complete the SHP-383 form.

NOTE: School districts have OCA designations which are used by DESE. When an ORI administrator requests a new user access, the levels available will include 1) ORI Read Only; 2) OCA Administrator 3) OCA Read Only. The options for OCA Administrator and OCA Read Only levels should not be used. For an exception to this rule, the school district MACHS administrator/LASO must contact the MSHP-CJISD Trainer/Auditor for assistance.

Law Enforcement Agencies - criminal justice agencies that have a noncriminal justice ORI for use with obtaining CHRI for noncriminal justice purposes, user access level will include:

- ORI Administrator and ORI Read Only
- Once the ORI Administrator is approved, the administrator can submit user requests for ORI Read Only.

Reminder: All user requests for an ORI Administrator with agencies assigned an ORI, or OCA Administrator for VECHS enrolled agencies, must be submitted on a MACHS User Access Form, SHP-383.

3.8.2 MACHS Administrator Responsibilities — Administrators are responsible for ensuring user access is kept current. User deletion requests must be submitted when the user is no longer affiliated with the agency, or their job function has changed and no longer requires access. Administrators are also responsible for ensuring Rap Back validations and Rap Back Hit notifications are acted on within the required and limited timeframe. Agencies may have more than one administrator level with one being the agency's designated LASO.

All users are responsible for reporting security incidents to their LASO. This includes unauthorized access to the portal through the use of credentials assigned to another user of the agency. Allowing unauthorized access is strictly prohibited and must be reported on an SHP-71, Security Incident Report form.

3.8.3 MACHS User Access Form (SHP-383) — This form is available on the MACHS portal under the documents section. This form contains personal identifiable information (PII). For the user's protection, email is not recommended unless encryption or password protection has been applied.

For assistance with user access, the MACHS Quick Reference Guide, SHP-368, is available on the MACHS portal.

3.8.4 MACHS Training for New Agency Access — Training is required for every agency prior to activation of a new ORI/OCA and for electronic access to CHRI via the Missouri Automated Criminal History System (MACHS). Training is conducted by a MSHP CJIS Trainer/Auditor and serves to ensure the agency LASO is made aware of the responsibilities associated with use and access of CHRI, fingerprint submission, and the resultant CHRI returned via MACHS or in hard copy. MACHS training consists of an overview of the MACHS portal user log-in procedures, MACHS portal navigation including, but not limited to, tracking registrations, viewing the CHRI, Rap Back hit notifications, and validation procedures. In addition, training includes access to CJIS Online for Security Awareness Training, applicant procedures for electronic, hard copy, or mail-in fingerprint submissions, information regarding secondary dissemination restrictions, and information on the Policy Compliance Review (PCR) process. Initial training is provided to the agency LASO and any other agency personnel. Future agency training of new agency personnel or MACHS users should be provided by the agency LASO and included in the agency's policy/procedure process.

SECTION 4: Security & Access

4.1 Guidelines For Access & 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, of Code of Federal Regulations (CFR). The III shall be accessed only for an authorized purpose. Furthermore, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.

4.2 Restrictions

CHRI is restricted to only those entities that have been determined to be qualified entities. Qualified entities are those entities authorized in state legislation pursuant to Public Law 92-544 and federal legislation (i.e. the Adam Walsh Act, the National Child Protection Act, as amended).

4.3 Retention/Storage Of CHRI/CJI

When CHRI is stored, agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. Retention of CHRI is not required by the MSHP-CJISD or FBI for audit purposes.

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 CHRI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. The agency shall, at a minimum, limit access to the controlled area during CHRI processing times to only those personnel authorized by the agency to access or view CHRI; lock the area, room, or storage container when unattended; and position information system devices and documents in such a way as to prevent unauthorized individuals from access and view.

4.3.1 Electronic Retention — Media protection policy and procedures shall be documented and implemented to ensure that access to electronic media is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting, and storing media.

The agency shall securely store electronic media within secure locations or controlled areas. The agency shall restrict access to electronic media to authorized individuals. If personnel restrictions are not feasible, then the data shall be encrypted. Encryption shall be FIPS 140-2 certified. (Refer to CJIS Security Policy, 5.10)

Electronic media means electronic storage media, including memory devices in laptops, 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.

Controls shall be in place to protect electronic media while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute other controls to ensure security.

4.3.2 Retention/Storage Off-Site — Procedures for handling and storage of information shall be established to protect the information from unauthorized disclosure, alteration, or misuse. The procedures shall apply to the handling, processing, storing, and communication of CHRI. These procedures apply to the exchange of CHRI no matter the form of exchange.

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Prior to storage of CHRI off-site and under the control of a third party, the agency is required to obtain an Outsourcing Management and Control Agreement. Outsourcing must be approved by the MSHP-CJISD, State Compact Officer, prior to any off-site storage.

4.3.3 Cloud/Electronic Retention of CHRI — The Missouri Automated Criminal History System (MACHS) allows an agency to house their criminal history responses indefinitely under the security protection of the MSHP, through a service called MACHS Retention. If not using MACHS retention provided by the MSHP CJIS Division, all electronic retention of CHRI must meet guidelines as stated in the CJIS Security Policy. If using cloud storage services, all cloud storage must be pre-approved by the MSHP/CJIS Division. Approved cloud providers pursuant to the MSHP Security Audit and Compliance Unit are: 1) Microsoft Azure Government Cloud, and 2) Amazon Web Services Government Cloud services. If electing to use cloud services, agencies must use the Government cloud offering as it meets CJIS Security Policy requirements. For questions or assistance, contact the MSHP CJIS Division. Asking questions in advance will help alleviate compliance issues with electronic or cloud storage.

As a reminder, contracting with a third party for storage, retrieval or destruction purposes, not with an approved cloud services provider as stated above, requires outsourcing approval by the MSHP State Compact Officer. Agencies must request permission to outsource prior to granting access of CHRI to a third party, as stated in Section 7 of this policy.

4.4 Destruction Of CHRI

It is recommended that on-site destruction be completed at the agency by authorized agency personnel. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

If an agency contracts with a private destruction company, the destruction must take place under the direct supervision of authorized agency personnel. If an agency allows destruction of criminal history records to occur off-site, a Management and Control Outsourcing Agreement is required. Approval must be granted by MSHP-CJISD prior to off-site destruction.

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. At a minimum, physical media should be cross shredded.

For electronic media destruction, the agency shall sanitize, that is, overwrite with random 0s and 1s at least three times or degauss the electronic media prior to disposal. Inoperable electronic 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.

4.5 Security of CHRI — Personnel Access to CHRI

Pursuant to CJIS Security Policy, Appendix J, agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment shall follow the guidance in the CJIS Security Policy which requires the submission of fingerprints. However, agencies located within states without this authorization or requirement are exempt from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

As a best business practice, the MSHP-CJISD recommends all individuals with access to CHRI have a fingerprint-based background check completed through the MSHP-CJISD and FBI.

4.6 Dissemination Of CHRI

Primary dissemination of CHRI is when the MSHP-CJISD disseminates to an authorized recipient. The MSHP-CJISD will not disseminate CHRI to the subject of record when the fingerprint submission and resultant CHRI is requested by an authorized recipient. Requests for secondary dissemination of CHRI must be obtained through the authorized recipient. The authorized recipient is under no obligation to disseminate.

Due to the sensitive nature of CHRI, secondary dissemination of CHRI by an authorized recipient should be limited. Dissemination is not authorized outside of Missouri. Agencies that have a commonality of purpose and (typically) congruent responsibility, authorized by federal statute or executive order, or state statute pursuant to Public Law 92-544, can receive CHRI and exchange that information with each other for the authorized purpose originally requested. The agencies must have a unity of purpose and typically, concurrent regulatory responsibility. Authorized recipients cannot share CHRI across state lines. There is no related agency or commonality of purpose across state lines.

The definition of CHRI is the results of a national fingerprint-based checks of criminal history records obtained through the FBI's NGI System for noncriminal justice purposes. Information is considered CHRI if it is transferred or reproduced directly from the CHRI obtained and is associated with the subject of record. Information is considered CHRI if it confirms the existence or nonexistence of CHRI.

Examples of dissemination methods include:

- correspondence such as letters and emails;
- documents such as forms and handwritten notes;
- conversations either in person or by telephone; and
- information in data fields such as spreadsheets

Authorized dissemination of CHRI includes:

- Dissemination from one agency to another agency when each agency has an approved Missouri ORI, approved pursuant to the same Public Law 92-544 legislation, and the CHRI's use is for the same purpose, such as employment, licensing. The corresponding use by a recipient must be authorized. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check.
- Dissemination to the subject of record for review and challenge purposes.

Dissemination Examples:

1. School District A receives a request from School District B for a copy of an applicant's background check. The applicant has applied at School District B and School District B

wants to view the background check results received by School District A. Is dissemination allowed?

Response: Yes. Dependent upon if School District A allows dissemination.

Both schools have an ORI and are approved under the same Public-Law 92-544 statute. A secondary dissemination log is required by School District A.

2. Agency A is a state agency with access to CHRI through a Public Law 92-544 statute for licensing purposes. Agency A receives a request for a copy of the background check from Agency B. Agency B is a VECHS approved agency whose authority is approved under the National Child Protection Act. Is dissemination allowed?

   Response: No. The criminal history was obtained under different legislation and for different purposes. Agency A received CHRI for licensing purposes under a Public Law 92-544 statute and Agency B has access under federal law, through the Missouri VECHS program. In addition, the purpose to use the CHRI is also different.

3. Agency A is a municipality with an ORI approved under Public Law for city employment. They receive a request from the subject of record for a copy of the background check. The subject of record wants to give the criminal history results to another agency for some other purpose. Is dissemination authorized?

   Response: No. Although dissemination to the subject of record is authorized, it is primarily for review and possible challenge purposes. A new background check should be requested for subsequent use. In addition, since Agency A receives CHRI through Public Law 92-544 legislation, a third party should not ask the subject of record to obtain a copy when they do not have the same authority. Agencies should refrain from disseminating CHRI to the subject of record when the purpose of the request is to further disseminate to another agency that does not have statutory authority to access CHRI. Agencies should be aware of anyone trying to circumvent the law.

4. Agency A is a state agency with an approved Public Law statute. Agency A has contracted with Agency B to perform eligibility reviews of CHRI on their behalf. Is dissemination authorized?

   Response: No. Access is not authorized unless Agency A enters in an outsourcing contract with Agency B. Outsourcing must be approved by the MSHP-CJISD State Compact Officer prior to access.

5. Agency A is a VECHS approved agency and receives criminal history for adoption/child placement purposes. The agency receives a request to view the results from other parties associated with the adoption process. Is Agency A authorized to disseminate to other parties?

   Response: No. The corresponding use by that recipient must be authorized. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check. For this example, the requesting parties would need to have the same access, i.e., be a qualified Missouri VECHS agency.

6. Agency A is an approved VECHS agency for adoption/child placement purposes. The Missouri court of jurisdiction over the adoption proceeding requests a copy of the CHRI. Is dissemination authorized?

   Response: Yes. The Missouri court has an ORI and has jurisdiction over the adoption. Agency

A is required to complete a secondary dissemination log and the court should be advised that the criminal history must not be disclosed in open court or further disseminated.

7. Agency A has a verbal conversation with the subject of record about the information reported in the CHRI results? Is dissemination authorized?

   Response: Yes. Verbal disclosure with the subject of record is authorized. A secondary dissemination log is required.

8. Agency A is a participating VECHS agency in Missouri and has a corporate office located outside of Missouri. The corporate office requires criminal history results be maintained in personnel files at the corporate office or uploaded electronically to the agency files maintained by corporate. Is this authorized?

   Response: No. All access to CHRI must be maintained in Missouri. For files stored in electronic medium, or cloud storage through corporate, agencies must follow procedures outlined in the CJIS Security Policy, Section 5.10. Access to encryption codes must be maintained and secured by the Missouri agency to ensure access to the CHRI is not accessible by other individuals located outside of Missouri.

4.6.1 Dissemination - Subject of Record — If agency policy permits, the officials may provide the applicant with a copy of the FBI criminal history record for review and possible challenge. If agency policy does not permit, the applicant may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding the process may be obtained from the FBI's website, https://www.fbi.gov/services/cjis/identity-history-summary-checks

It is important to note that agencies are under no direct obligation to disseminate CHRI to the subject of record and dissemination should be limited for review and possible challenge purposes.

When dissemination is with the subject of record, an agency must verify the subject's identity prior to dissemination and keep a secondary dissemination log for each occurrence. In order to limit potential risks associated with a subject's subsequent use of a criminal history record, an agency may wish to consider marking the record in some manner to distinguish it as a copy and not an original. As a best business practice, the original CHRI response should remain with the agency and a copy may be provided to the subject of record.

CHRI may not be disseminated to spouses or other household or family members, even at the subject's request. Furthermore, CHRI may not be disseminated to other parties such as potential employers on behalf of the subject.

4.6.2 Dissemination - Public Hearing/Access — CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates: 1) the hearing is based on a formally established requirement; 2) the applicant is aware prior to the hearing that CHRI may be disclosed; 3) the applicant is not prohibited from being present at the hearing; and 4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process.

For example, a board or commission with access to CHRI, may hold regularly scheduled meetings where applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large.

Dissemination Reminder:

- Do not disseminate CHRI outside of Missouri.
- Do not disseminate to a relative, family members, or friends of the subject of record.
- Do not disseminate to unauthorized agencies.
- Do not disseminate CHRI to a regulatory auditor. Refer to section 4.6.3.

4.6.3 Dissemination/Access of CHRI by Regulatory Auditors — An agency is under no obligation to disseminate CHRI to any agency when the CHRI was obtained through the systems of the MSHP-CJISD and FBI. If agency policy permits dissemination, all access to CHRI or dissemination requested by a regulatory auditor must be submitted to the MSHP-CJISD for approval. The regulatory auditor must provide the agency with detailed information explaining the type of audit being conducted, the purpose, and use of CHRI in relation to the audit. The agency must forward the request to the MSHP-CJISD for review. The MSHP-CJISD has sole authority to approve or deny access to CHRI for regulatory auditors.

Examples of CHRI requests by a regulatory auditor may include:

Example 1: *Verification that a "background check" was completed. The background check definition must be specific. Is it for open records or closed records? If the request consists of open records, obtained from Missouri CaseNet or the MACHS Name-Search Portal, the MSHP-CJISD has no concerns with an agency disclosing open record information they obtained from open record databases.*

Example 2: *Verification that a fingerprint-based background check was conducted by the agency. For fingerprint-based CHRI, which consists of Missouri closed records and FBI CHRI, the agency may give the regulatory auditor clearance information. Clearance information consists of name of applicant, date of the completed criminal history, and if the applicant was deemed eligible or ineligible by the agency. Since the clearance information does not contain personally identifiable information (PII), or CHRI obtained from the MSHP-CJISD and FBI, the MSHP-CJISD has no concerns with this practice.*

Example 3: *Access (to view and make use of) of the fingerprint-based CHRI. The regulatory auditor is requesting access to the fingerprint-based CHRI that the agency received from the systems of the MSHP-CJISD and FBI. All requests for access to CHRI by regulatory auditors must be reviewed by the MSHP-CJISD prior to dissemination or access.*

Failure of an agency to receive approval from the MSHP-CJISD prior to granting access to a regulatory auditor will be deemed as unauthorized dissemination and may jeopardize the agency's access to CHRI. All unauthorized dissemination will be documented in a Security Incident Report, SHP-71.

For requests received from an agency to allow access to CHRI by a regulatory auditor, the MSHP-CJIS will provide a decision of approval or denial within 15-30 days of receipt of the request.

For approvals granted by the MSHP-CJISD, the agency will be advised and must adhere to the following requirements:

1. The agency LASO will obtain a current Security Awareness Training (SAT) certificate from the regulatory auditor(s) prior to access, pursuant to guidelines in the CJIS Security Policy;
2. The agency LASO will document in a secondary dissemination log, each record result viewed by the regulatory auditor(s);
3. The agency LASO will monitor each record viewed by the regulatory auditor(s), and ensure CHRI is not copied or removed outside of agency files; and

4. The agency LASO will maintain the SAT certificate(s) and the secondary dissemination log for a minimum of 3 years or until a PCR has been conducted by the MSHP-CJISD.

4.6.4 Where does it say that records can only be used for the purpose for which they were requested? — There are multiple references which state that a criminal history record may be used only for the official purposes for which the record was requested. Those include, but are not limited to the following:

- The National Crime Prevention and Privacy Compact Act, Title 42, United States Code, Section 14616, Article IV(c) - "Any record obtained under this Compact may be used only for the official purposes for which the record was requested."
- Title 28, Code of Federal Regulations (CFR), Section 50.12 (b) - "Records obtained under this authority may be used solely for the purpose requested..."
- Title 28 CFR Section 20.33 (d) - "Criminal history records received from the Interstate Identification Index (III) System or the Fingerprint Identification Records System (FIRS) shall be used only for the purpose requested..."
- Criminal Justice Information Services Security Policy (CJIS Security Policy) - CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed."

4.7 Dissemination Log Standards

Secondary dissemination occurs when a criminal history is passed from the receiving agency to another agency, or subject of record. In order for dissemination to be authorized to a would-be recipient, the corresponding use by that recipient must be authorized. As with the use of CHRI, parameters for dissemination are derived from the specific federal statutory authority leveraged to obtain CHRI. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check.

When secondary dissemination occurs, the disseminating agency must log each occurrence. The copy should be marked as "copy" and the secondary dissemination log must be retained by the disseminating agency for a minimum of 3 years or until the agency has received a PCR from the MSHP-CJISD.

Agencies are encouraged to develop a procedure and/or agency policy on dissemination to include method of dissemination, and the completion and retention of secondary dissemination logs.

Examples of dissemination methods include:

- Verbal disclosure with the subject of record, or authorized agency;
- In person conversation with the subject of record, or authorized agency;
- U.S. Mail to the subject of record, or authorized agency;
- Email or Facsimile (Fax). As a reminder, do not email or fax CHRI to authorized recipients unless protection is applied to the document, i.e., encryption or password protection.

The following is the established minimum standard for a secondary dissemination log for noncriminal justice purposes. The log must contain:

1. The name of the subject of record/applicant;
2. The name of the person and/or agency requesting the record;
3. The purpose for the request;
4. The name of the person releasing the record;
5. The date released;
6. Signature of the person receiving the record, when dissemination is in person.

Examples of the types of secondary dissemination logs include:

1. The agency may develop and use a standardized hard copy or electronic dissemination log;
2. The agency may log by way of written correspondence and maintained in agency or employee files, such as copy of the approval/denial letter, notations on application, etc.

4.8 Misuse Of CHRI

Section 43.540.5 RSMo Any information received by an authorized state agency or a qualified entity pursuant to the provisions of this section shall be used solely for internal purposes in determining the suitability of an applicant. The dissemination of criminal history information from the Federal Bureau of Investigation beyond the authorized state agency or related governmental entity is prohibited. All criminal record check information shall be confidential and any person who discloses the information beyond the scope allowed is guilty of a class A misdemeanor.

Section 43.532 RSMo Criminal history and identification records obtained from the Central Repository shall be used solely for the purpose for which they were obtained. The subject of the record shall be afforded the opportunity to challenge the correctness, accuracy, or completeness of a criminal history record.

The Central Records Repository shall have authority to engage in the practice of collecting, assembling, or disseminating CHRI for the purpose of retaining manually or electronically stored criminal history information. Any person obtaining CHRI from the central repository under false pretense, or who advertises or engages in the practice of collecting, assembling, and disseminating as a business enterprise, other than for the purpose of furnishing criminal history information to the authorized requester for its intended purpose, is guilty of a class A misdemeanor.

Section 576.050 RSMo A person commits the crime of misuse of official information if he or she knowingly or recklessly obtains or discloses information from the Missouri Uniform Law Enforcement System (MULES) or the NCIC or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job. Misuse of official information is a class A misdemeanor.

What United States Code (U.S.C) or Code of Federal Regulations (CFR) covers the misuse of Criminal History Records?

The misuse of criminal history records are covered by various federal statutes and regulations included, but not limited to the following:

Title 28 United States Code (U.S.C.), section 534, Public Law 92-544, and Title 28 CFR section 20.33(b), provide that the exchange of records and information is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies. Further, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Depending on the authority to which the CHRI was authorized for dissemination, penalties may be different according to the authority.

The Privacy Act, Title 5 U.S.C. Section 552a(i)(3) "any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000."

Title 18 U.S.C. Section 1030(c), In summary, there are several criminal penalties, such as fines and/or imprisonment, referenced in the Fraud and Related Activity in Connection with Computers section, which may be imposed for knowingly or intentionally accessing a computer and obtaining information without authorization or exceeding authorized access.

Title 28, Code of Federal Regulations, Section 907.4(b)(4), "If the Compact Council agrees with the Sanctions Committee's finding, the Compact Council Chairman or the FBI Director or Designee shall direct the FBI Compact Officer to take appropriate action to suspend noncriminal justice access to the III System by the offending agency. If the offending agency is a criminal justice agency, the Compact Council Chairman shall request the Director of the FBI to take appropriate action to suspend noncriminal justice access to the III System by the offending agency."

In addition, other federal statutes pertaining to background checks, such as the Nursing Home Act, gives specific penalties for misuse of information.

SECTION 5: Security Awareness Training

5.1 Security Awareness Training Overview

Basic security awareness training shall be required at initial assignment and renewed annually for all personnel who have access to criminal justice information (CJI). Access to CJI includes direct access or access to CJI through fingerprint submission. Security Awareness Training must be completed through CJIS Online (cjisonline.com). For questions on access to the training link, you must contact your regional CJIS Trainer/Auditor.

CJI is any information collected by the FBI, MSHP, or other criminal justice entities. It is available to anyone who is authorized to use CJIS systems. CJI is not limited to criminal history or information available through MULES, and includes personally identifiable information (PII) and other derived information.

The responsibility of each agency and person with access to CJI is to know that the information contained within the CJIS information systems is sensitive information. Improper access, use, and dissemination of CJIS data is serious and may result in the imposition of administrative sanctions including termination of services, as well as state and/or federal criminal penalties. Each person with access to CJI has a responsibility to protect the information and report security incidents.

5.1.1 What Happens If A Person Misuses CJI? A person commits the crime of misuse of official information if he or she knowingly obtains or recklessly discloses information from the MULES or the NCIC, or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job. Misuse of official information is a class A misdemeanor.

Disseminating or sharing CJI with anyone that is not authorized to have access to the information is strictly prohibited. All CJI must be protected from creation through destruction.

Agencies are required to have a Security Incident Response Plan and use a Security Incident Response form (SHP-71) to report violations. For agencies with MACHS portal accounts, both are available in the documents section.

Security incidents within an agency are typically reported to the agency LASO. However, in the absence of the LASO, any individual may report incidents up their chain-of-command, or to their entity head who must report to the MSHP-CJISD or the CJIS Trainer/Auditor assigned to their agency.

The LASO is responsible for:

- Maintaining the list of users who have access to CJI.
- Identifying how equipment is connected to MSHP-CJISD (if applicable).
- Ensuring proper personnel screening procedures are being followed, such as fingerprint background check of personnel having access to CJI. This is a best business practice for agencies that access CJI for noncriminal justice purposes.
- Notify MSHP-CJISD of any security incidents using the Security Incident Report form, SHP-71.

5.1.2 Media Protection & Disposal — The protection must include both physical and electronic media and includes Flash Drives, Hard Drives, CD, DVD's, documents, pictures, etc. All media must be stored in secure areas and should be granted to authorized personnel only. Make sure that printed information is printed to the correct printer. All CJI data located, transmitted, or transported outside a secure location must be encrypted, according to FBI standards, or carried in a locked container and protected in transit. When in transit, it should be carried in locked container or folders where it is not visible to the public. When destruction is necessary, electronic media must be physically destroyed or overwritten three times and shredded or incinerated.

5.1.3 Physical Security Of CJI — In order to handle or process CJI, staff and equipment must be in a secure location. The location could be a building, room, or area, and the area should be marked. A list of authorized users must be maintained. The area must have controls such as locks. Monitors and printers must be secure in order to prevent unauthorized viewing of CJI.

5.1.4 Threats — Be aware of the different types of threats, which include (a) natural threats, (b) unintentional threats, and (c) intentional threats. A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system. Threats can come for internal or external sources and vulnerabilities lead to threats. Further explanation of threats is as follows:

- Natural threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning. Natural threats include fire, flood, lightning, and power failures.
- Unintentional threats are actions that occur due to lack of knowledge or through carelessness. These threats can be prevented through awareness and training. Unintentional threats include physical damage to equipment, deleting information, and permitting unauthorized users to access information.
- Intentional threats are those threats that are deliberately designed to harm or manipulate an information system, its software, and/or data. Security software such as an antivirus program is designed to protect against intentional threats. Intentional threats include social engineering, phishing, sabotage, eavesdropping, unauthorized data access, intrusions, denial of service, theft, etc.

5.1.5 Password Policy For CJI — Your agency's password policy should be a minimum length of eight characters. It cannot be a dictionary word or proper name and cannot be the user ID. The password should be set to expire every 90 days and cannot be identical to the previous 10 passwords. It cannot be displayed when entered. Each person with access should be advised to not share their password with anyone, including the agency IT staff. Passwords should not be written down and do not use increment numbers in the passwords. Do not make it easy to type or use keyboard patterns. Some hints for good passwords are to use phrases or run words together. Substitute special characters for common letters ($0somethingeasy2remember.)

5.1.6 Email & Email Attachments — Email is NOT a secure method of communication. As a general rule, do not send anything in an email that you do not want others to see. Do not send CJI in an email unless you know that proper technical controls are in place to protect it, such as encryption and access control. All email should be scanned for known viruses and spam, but it is still an easy avenue for malicious code.

5.1.7 Internet Policy — Internet should be monitored and controlled. All devices that connect to the Internet should be protected by a firewall.

5.1.8 Social Engineering — The attempt to gather information by deception. Scams and phishing attempts are the major categories of social engineering. Social engineering could come from any source such as email, telephone, or face-to-face communication. It will not be obvious that the person is trying to gather information and could be masked as a marketing call. If you are suspicious, do not answer and report the incident. Never respond to an email asking for personal or confidential information, especially if it comes from someone you do not know.

5.1.9 Laptop, Handheld, & Personal Devices — There are many personal and work-related devices available. Each user should know the agency policy of using these devices. Personal devices are NOT allowed to access CJI systems. Devices need to be secure and managed by the agency IT staff and need to be password protected and encrypted. If lost or stolen, report it as an incident. Laptops must be encrypted. Lock the computer before stepping away from the work area. CJI should not be stored, accessed, or viewed from personal computing equipment, and should not be accessed from a library, school, or hotel computers.

5.1.10 Access Requests — The access request process should be a documented process. The main focus is separation of duties and least privileged access. A person who authorizes access should not have the ability to implement the request. The level of access should be enough to perform the job duties. Do not give higher authority to a person unless needed. If your user ID is compromised and you have the least level of access, less information is at risk.

5.2 Security Awareness Training Online Resource

Pursuant to the CJIS Security Policy, basic security awareness training (SAT) shall be required within six months of initial assignment, and biennial thereafter, for all personnel who have access to CHRI, to include all personnel who has unescorted access to a physically security location. Agencies must ensure all personnel with access to CHRI have a current SAT certification on file. All training must be conducted through CJIS Online.

The Local Agency Security Officer (LASO) of an agency actively represents their agency in all matters pertaining to information security and access to CHRI. The LASO is responsible for ensuring all personnel with access to CHRI have current training certificates on file. The LASO training is conducted through CJIS Online and is required annually.

SECTION 6: Policy Compliance Review (PCR)

6.1 Background

The CJIS Security Policy provides the minimum standard requirements for states to follow. The states, by policy, may adhere to the minimum standards or choose to be more restrictive, but they cannot be less restrictive. In December 2002, the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) recommended that the FBI CJIS Audit Unit begin auditing Noncriminal Justice Agencies (NCJAs) that receive FBI CHRI via applicant fingerprint processing. The FBI CJIS Audit Unit began conducting pilot audits on these agencies in 2004, and in October 2008, began to permanently conduct noncriminal justice agency audits.

With this new requirement, the APB approved a section in the CJIS Security Policy to include a state requirement to audit noncriminal justice agencies with indirect access to III system information. The requirement stated:

"The appropriate, authorized state official, which may be the CJIS systems officer, the state compact officer, or the state repository director, shall periodically conduct audits of the state's noncriminal justice agencies with indirect access to III information through the submission of fingerprints." (U.S. Department of Justice, FBI, *Informational Letter Regarding State Noncriminal Justice Agency Audits*, dated Feb. 9, 2009.)

The FBI CJIS Security Policy, Appendix J requires that "states shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs."

In addition, CSAs shall, in coordination with the SIB (SIB), establish a process to periodically audit all NCJAs with access to criminal justice information in order to ensure compliance with applicable statutes, regulations, and policies.

In Missouri, the process of periodically auditing all NCJAs with access to criminal justice information (CJI) is the responsibility of the MSHP-CJISD. Thus, in 2009 and in response to the APB, the MSHP-CJISD developed the noncriminal justice audit program with designated NCJA auditors. The NCJA audits, referred to as PCRs, are conducted with each agency on a triennial basis. Generally, the first PCR is conducted within the first year of access and triennial thereafter. Reviews may be conducted more frequently than the standard three years, and an agency may request a review any time the point contact believes it would be beneficial to their agency. Such requests should be directed to the regional CJIS Trainer/Auditor.

6.2 Areas Of Review

- Local Agency Security Officer/Point Of Contact
- User Agreement
- Access and Use Of CHRI
- Fingerprint Submission Policy
- Dissemination Practices/Policy
- Retention/Storage Policy
- Destruction Policy

- MACHS User Access List
- Waiver Agreement & Statement, for VECHS agencies
- Security Awareness Training Certificates
- Rap Back Participation, Rap Back Hits and Validation Procedures, if applicable
- Outsourcing Approvals, if applicable

6.2.1 Local Agency Security Officer (LASO) — The LASO serves as the primary point of contact between agency and the MSHP-CJISD. The LASO actively represents their agency in all matters pertaining to information security of criminal history.

6.2.2 User Agreement — Per the CJIS Security Policy, each agency with access to CJI must have a current and valid user agreement.

6.2.3 Use & Access Of CHRI — An agency will be assessed for compliance regarding the use and access to the CHRI. Compliance assessment includes the verification that the agency is using the CHRI for the purpose for which it was obtained. The purpose and use must be in accordance with the authority of the agency. The authority is based on the ORI approval and the state or federal law that granted access to CHRI.

Access to CHRI is based on fingerprint submission and is tracked by the MSHP-CJISD with dissemination logs for an agency ORI or ORI and OCA. The fingerprint submission (or data sampling) will show a list of records that the requesting agency has received. The data sampling may include 25 record requests and may include a timeframe from the previous 3 years to the current date. An additional sampling beyond 25 records is authorized if deemed necessary.

Generally, PCRs are scheduled with the agency approximately six weeks in advance; however, the MSHP-CJISD reserves the right to make unannounced visits.

Things to consider regarding access to CHRI:

1. Is the criminal history record being requested on an individual affiliated with the requesting agency and for an authorized purpose, i.e., employment, volunteering, licensing?
2. Does the purpose match the authority identified in the state law or federal law?
3. If the agency is a VECHS agency, was the applicant given the Waiver Agreement and Statement prior to being asked to submit fingerprints? Is the agency retaining a copy of the signed waiver?
4. Is the criminal history response from the MSHP/FBI being disseminated to another agency or person? Before granting access through dissemination, you must first ensure that access or dissemination is authorized. Please remember, access can be in many forms, i.e. verbal, written, electronic, email, or facsimile, and must be authorized.

Reminder: *Any use of CHRI outside of the authorized purpose as stated in either state statute or the federal law is strictly prohibited and may be deemed as "misuse" and is subject to state and federal criminal and civil penalties.*

6.2.4 Fingerprint Submission Practices — Each agency should have a policy or procedure in place for fingerprint submission practices. The MSHP accepts both hard copy fingerprint cards and electronic fingerprint image and data submission.

6.2.5 Suggested Chain Of Custody Procedures For Fingerprints — An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the Central Repository (MSHP). The following information provides a guide to developing a chain of custody process:

- Establish provisions for the agency to manage both manually and electronically captured fingerprints.
- Establish an agency tracking system or applicant log using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity.
- Establish a procedure that documents the type of identification used by the applicant.
- Establish procedures that use special sealed envelopes, agency specific stamps, etc., for the agency to use when forwarding the applicant's manual fingerprint card.
- Implement the use of forms that may include the date of fingerprinting, reason, the name of the applicant, etc.

6.2.6 Dissemination Practices — Each agency will be assessed on dissemination practices. For agencies that allow dissemination to another agency, or to the subject of record, procedures must be followed to ensure compliance with state and federal law. For this reason, each agency should have a policy or procedure in place outlining their dissemination practices.

6.2.7 Retention & Storage Policy — Each agency will be assessed on retention practices. CJI may be destroyed at which time it is no longer needed. CJI is not needed for audit purposes since the MSHP-CJISD keeps a dissemination record of all CJI disseminated to all agencies.

For audit purposes, the agency is required to keep supporting documentation that substantiates the legal authority or purpose for requesting the CJI (i.e. an employment application, applicant file, waiver form, or some other type of document that proves the applicant applied for, retained a position at, or received some type of benefit from the agency.) If unable to provide supporting documentation, the request for CJI may be deemed as unauthorized.

If your agency policy is to retain the CJI, it must be kept in a secure records environment and free from public or unauthorized access. The area must be secured by lock and have limited access. If CJI is retained in electronic media, the data must be protected and not accessible from outside the agency or across state lines. If storage of CJI is off-site and under the control of a third party, the agency will be required to obtain an Outsourcing Management and Control Agreement prior to allowing a third party access or storage responsibilities of the CJI.

6.2.8 Destruction Policy/Practices — Each agency will be assessed on destruction of CJI, if destroyed. It is recommended that destruction be completed on-site at the agency by authorized agency personnel and in a manner that is acceptable to CJIS Security Policy. If your agency contracts with a private destruction company, the destruction must take place under your agency's direct supervision. If any agency allows destruction of CHRI to occur off-site, an Outsourcing Management and Control Agreement is required prior to access.

6.2.9 Waiver Agreement & Statement — (VECHS agencies only) — The Waiver Agreement & Statement (SHP-981) is a form required by all VECHS agencies only. The Missouri VECHS program is a MSHP program approved by the FBI through federal legislation and administered by the CJIS Division. The Waiver Agreement & Statement adheres to the FBI requirement of Title 28, 16.30-34 and is auditable. Each VECHS entity is required to produce the waivers during the PCR. Failure to obtain waivers from the applicant prior to requesting CHRI may subject the agency to civil liabilities. For

audit purposes, the agency may be assessed as noncompliant, which may require a follow up audit and could also result in suspension of access to CHRI.

6.2.10 Security Awareness Training (SAT) will be reviewed to ensure individuals with access to CJI have completed the required training. Basic SAT is required within six months of initial assignment, and biennial thereafter. Access to CJI includes direct access or access to CJI through fingerprint submission. SAT is available online with training and testing.

6.2.11 Outsourcing will be discussed with the agency to ensure agency personnel are aware of what constitutes as outsourcing. When an agency is allowing a third party to have access to CJI in any form, the agency must have an approved outsourcing standard in place.

Examples of unauthorized outsourcing include, but not limitied to:

1. Allowing a third party to handle destruction off-site or unsupervised;
2. Storing agency files containing CJI off-site under the control of a third party;
3. Retaining electronic CJI on a server that is accessible by third parties;
4. Contracting with a third party for administrative services to view and make eligibility determinations.

6.2.12 Rap Back Program Participation will be reviewed. For participating agencies, this will include a review of requested Rap Back hit notifications, and validation procedures.

6.3 PRE-REVIEW PREPARATION PROCESS FOR PCRs

The CJIS auditor will review the agency information and contact the agency POC approximately six weeks prior to the on-site review to gather or confirm basic information regarding the agency's use of CHRI. During this initial contact, the CJIS auditor will provide an overview of the audit and verify agency information, i.e., agency location, parking, access to building.

6.4 ON-SITE AGENCY REVIEW PROCESS

6.4.1 Administrative Interview — At the pre-arranged time, the CJIS auditor will conduct the on-site portion of the agency review. During this portion, the LASO should be present. The administrative interview is used to determine whether agency CHRI policy and procedures for receipt of state and FBI criminal history are in accordance with state and federal law.

6.4.2 Data Quality Review — In conjunction with the interview, a data quality review is conducted of the CHRI requested/received by the agency based on their authority. The data qualify review will include factors such as a) was the request for CHRI authorized based on the authority granted to the agency; b) what was the purpose for requesting CHRJ, i.e., employment, licensing; c) what is the agency's retention, destruction, security and dissemination policy relating to the receipt and use of the CHRI requested/received; d) does the agency have documentation on file that substantiates the applicant is/was under their purview at the time of requesting/receiving CHRI.

Agencies must ensure they have supporting documentation on file that verifies the applicant is under their purview prior to receiving CHRI. This is to ensure they are receiving criminal histories for individuals who can be accounted for. To help alleviate the chances of receiving criminal histories for unknown individuals, it is highly recommended that the agency does not provide fingerprint instructions (such as their MACHS fingerprint registration code) to their applicants until they have an application or some other type of notification document on file that will substantiate the applicant is under

their purview. Typically, applications for employment or licensure are the primary forms of documentation. Agencies are responsible for maintaining documentation for audit purposes, and to ensure they can account for every individual to which a criminal history is requested/received.

For example, noncompliant data may be classified as follows:

- ***Unauthorized Request*** — CHRI was requested without legal authority; requesting CHRI for another purpose outside the scope allowed in statute or law; failing to provide supporting documentation to auditor that substantiates the request for CHRI.
- ***Unauthorized Dissemination*** — CHRI disseminated to an unauthorized person or agency; CHRI disseminated out of state; CHRI stored on a company server or website that is accessible to others not authorized to have access or view.
- ***Unsecure Location For CHRI*** — CHRI maintained in open cabinets; CHRI maintained electronically without proper technical safeguards; CHRI stored electronically or in hard copy form in an unrestricted environment.
- ***Fingerprints Not Submitted*** — This category is applicable to agencies required by state or federal law to submit fingerprints on applicants for specific purposes, i.e. concealed carry permits, housing applicants, emergency child placements.
- ***Failure To Submit Fingerprints In A Timely Manner*** — This category specifically applies to the DSS Children's Division and Juvenile Office for emergency child placements.

6.4.3 Exit Briefing. The purpose of the exit briefing is to present the findings of the review to the LASO or agency representative. The formal summary and findings document may be left with the agency at the time of the PCR, or the CJIS auditor may complete the findings and electronically send the document to the LASO or agency representative, at a later date. Generally, the electronic summary and findings document is sent via email to the agency LASO within 15 business days following the completion of the review. Hard copy documents are also available and will be mailed if agency prefers. The audit may require a follow-up which will be conducted within 90 days to address any areas of concern, or those items deemed noncompliant. If the areas of concern have been satisfied during the follow-up review, no further action will be required.

6.5 Agency Requirement For Noncompliance Findings

For all areas of concern or those deemed noncompliant, the agency LASO is required to provide a written response to the MSHP-CJISD within 30 days after the PCR completion date. The response letter should include a plan of action that will place the agency within policy guidelines. Upon completion of the corrective measures, the agency head or POC must notify the MSHP-CJISD in writing that the agency has accomplished its planned objectives and is now in full compliance with policy and regulations.

If the agency LASO fails to provide the MSHP-CJISD with a plan of action, the agency will be considered noncompliant and will be subject to access suspension. If an agency refuses to cooperate in an agency/MSHP-CJISD audit, the agency will be considered noncompliant and access to CHRI will be suspended.

SECTION 7: Security & Management Control Outsourcing Standard

To assist agencies with outsourcing, this section provides a summary of the requirements and responsibilities of both the authorized recipient and contractor. The provisions of the Security and Management Control Outsourcing Standard (Outsourcing Standard) are established by the Compact Council pursuant to Title 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the authorized recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network.

As a summary, the information contained in this section is not all inclusive and agencies are instructed to read, in full, the Outsourcing Standard document. A complete copy is available in Appendix E of this manual, along with links to the MSHP and FBI website.

7.1 What Is Outsourcing?

Outsourcing is a term heard frequently in recent years referring to the delegating of a function to an independent provider. In the realm of criminal justice, this refers to a specific type of outsourcing that involves access to confidential and restricted information obtained from the systems of the MSHP and FBI.

Authorized recipients of CHRI may have the need to outsource some responsibilities to an outside agency or third-party contractor. In terms of outsourcing duties as they relate to CHRI, this may include an authorized recipient contracting with a third party to review the background check results and make the eligibility or hiring determinations, storage of personnel files containing criminal history records, and destruction procedures. In addition to hard copy access to criminal history records, outsourcing also applies to electronic media. There is an increasing occurrence of record information being maintained electronically and accessed by information technology vendors and contractors.

Prior to allowing a third-party contractor access to criminal history records, an Outsourcing Standard must be approved by the MSHP-CJISD and state compact officer.

Outsourcing of noncriminal justice administrative functions from the authorized recipient to a contractor includes, but is not limited to, the following:

1. Making fitness determinations and/or recommendations;
2. Obtaining missing dispositions;
3. Disseminating CHRI as authorized by federal statute, federal executive order, or state statute;
4. Other authorized activities relating to the general handling, use, and storage of CHRI.

7.2 What Is An Outsourcing Agreement? When Is It Needed?

The National Crime Prevention and Privacy Compact Act of 1998 established the infrastructure that allows states to share information for noncriminal justice purposes. It also created the Compact Council which serves as the governing body that establishes the rules and procedures regarding access to III.

CHRI is confidential and must be protected from creation through destruction. In order to address issues of outsourcing, the Compact Council enacted the *Security and Management Control Outsourcing Standard for Non-Channelers.* The purpose of the Outsourcing Standard, in part, is to provide adequate security and integrity for CHRI while under the control or management of an outsourced third-party, the contractor. It also requires the contractor have in place the proper security program that will ensure the integrity of information obtained is not compromised and meets all requirements of state and federal laws, FBI CJIS Security Policy, and the United States attorney general.

To ensure the contractor adheres to all security procedures, the authorized recipient must enter into a contract with the third-party contractor specifying the exact duties of the contractor as outlined in the Outsourcing Standard document.

The Compact Council has the authority to suspend or terminate the authorized recipient's exchange of CHRI if the authorized recipient fails to notify the state compact officer of any security violations, or refuses to or is not capable of taking corrective action in resolving the security violations. If CHRI has been suspended, it may be reinstated pending written verification from the authorized recipient, the contractor, and the state compact officer to the Compact Council or the United States attorney general that the security violation has been successfully resolved. If access to CHRI has been terminated with the authorized recipient, then the contractor's records containing CHRI must be deleted or returned with the appropriate time frame as specified by the authorized recipient.

In view of the stringent requirements for security and concern for any unauthorized access to CHRI, the authorized recipient must be assured that the contractor is capable of adhering to all technical and procedural security requirements per the FBI CJIS Security Policy before outsourcing any functions requiring access to CHRI to a contractor.

7.3 Steps Required Prior To Implementing Outsourcing

Outsourcing is restricted between governmental entities. For outsourcing eligibility review, an authorized recipient (governmental or nongovernmental) must:

1. Contact the MSHP-CJISD and/or State Compact Officer prior to granting access of CHRI to a contractor.
2. Provide information, or draft an outsourcing contract, listing the specific duties to be performed by the contractor that pertain to access and use of CHRI.

NOTE: Access to CHRI by an outside entity/contractor without approval from the MSHP-CJISD and State Compact Officer is strictly prohibited. Agencies granting unauthorized access to CHRI may be subject to state and federal penalties.

7.4 Sample Contract Wording

"This contract is entered into between [insert authorized recipient's name and address], the authorized recipient, and [insert contractor's name and address], the contractor, under the terms of which the authorized recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of CHRI pursuant to Title 28, Code of Federal Regulations, Part 906 and the relevant Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard), and the relevant CJIS Security Policy. The most current version of the Outsourcing Standard and CJIS Security Policy are incorporated by reference into this contract and appended hereto as Attachments [insert attachment #].

The authorized recipient's authority to submit fingerprints for noncriminal justice purposes and to obtain the results of the fingerprint search, which may contain CHRI, is [insert the legal citation of the state statute]. This authority requires or authorizes fingerprint-based background checks of [insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by state statute].

The specific noncriminal justice administrative function(s) to be performed by the contractor that involve access to CHRI on behalf of the authorized recipient is to [insert specific noncriminal justice administrative functions to be performed, e.g., obtaining missing dispositions, making fitness determinations and/or recommendations, storing of or destruction of criminal history record check results].

[Insert contractor's name] will comply with the Outsourcing Standard requirements, CJIS Security Policy, and other legal authorities to ensure adequate privacy and security of personally identifiable information and criminal history record check results related to this contract, and will ensure that all such data is returned to the authorized recipient when no longer needed for the performance of contractual duties."

A copy of the signature page with dates must be included with the contract.

SECTION 8: Fingerprint Submission

8.1 Fingerprint Submission To The MSHP-CJISD

There are two options for fingerprint submission to the MSHP-CJISD:

1. Electronic Fingerprint Submission — MACHS Website/State Fingerprint Vendor
2. Manual Fingerprint Submission — Using the Applicant Fingerprint Card (FD-258)

Several agencies require specific fingerprint submissions. For instance, they may require that applicants use the Patrol's MACHS website for fingerprint registration and electronic fingerprint capture through the state's fingerprint vendor. Agencies are responsible for providing fingerprint instruction to their applicants.

8.1.1 OPTION 1: MACHS Website For Registration — MACHS is administered by the MSHP-CJISD. Each entity with an approved ORI is assigned a four-digit MACHS registration number to use with the applicant registration process for electronic submission of fingerprints. The MACHS number is specific to the agency ORI and ensures that the criminal history record responses are disseminated to the authorized recipient.

MACHS Website: www.machs.mo.gov

Each agency is responsible to provide the MACHS registration number to their applicants prior to fingerprinting. Agencies must ensure that their applicants understand the proper use of the MACHS registration number. Using a wrong number will result in the state and FBI responses being sent to another agency. The MACHS website has several safeguards in place that prompts the applicant to verify the information entered. However, if the information is not verified and results are sent to an unintended agency, the applicant will be required to begin the process over and may incur additional fees.

The state fingerprint vendor does not have access to CHRI. Any questions regarding background check results must be referred to the requesting agency.

8.1.2 OPTION 2: Manual Fingerprint Submission — Using FD-258 Applicant Fingerprint Card. Local law enforcement agencies and the state fingerprint vendor may assist the public with fingerprint cards. Applicants should check with their local law enforcement to verify if fingerprinting services are available.

8.1.3 Out-Of-State Applicants — Agencies may advise their applicants to use the MACHS registration process and select the "out of state" applicant option.

8.2 Fingerprint Fees

All fees for CHRI provided by the MSHP-CJISD and FBI are in accordance with section 43.530 RSMo and Title 28 Code of Federal Regulations 20.31(e)(3).

8.3 Fingerprint Submission, Chain Of Custody (Best Practice)

The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state, and federal governmental officials, which prescribes system rules and procedures for the effective and proper operation of the III for noncriminal justice purposes. The demand for fingerprint-based background checks for noncriminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. Based on the Compact Council's Best Business Practice, it is recommended to request and obtain photographic identification when capturing an individual's fingerprints. Do not provide the fingerprint card to the applicant to submit, as the applicant could alter the card.

8.3.1 Primary & Secondary Identification — Most agencies request some type of photo identification card as one method for verifying an individual's identity. The Compact Council suggests agencies accept only current, valid, and unexpired picture identification documents. As a primary form of picture identification, an applicant may present a state-issued driver's license, which meets the requirements of Public Law 109-13 when being fingerprinted. However, in the absence of the driver's license, applicant may provide one or more secondary documents including:

- State Identification Card (if the state's identification card standards are the same as the driver's license);
- State Government Issued Certificate Of Birth;
- U.S. Active Duty/Retiree/Reservist Military Identification Card;
- U.S. Passport;
- Federal Government Personal Identity Verification Card;
- Department Of Defense Common Access Card;
- U.S. Tribal Or Bureau Of Indian Affairs Identification Card;
- Social Security Card;
- Court Order For Name Change/Gender Change/Adoption/Divorce;
- Marriage Certificate (Governmental Certificate Issued);
- U.S. Government Issued Consular Report Of Birth Aboard;
- Foreign Passport With Appropriate Immigration Documents;
- Certificate Of Citizenship;
- Certificate Of Naturalization;
- INS Resident Alien Card (issued since 1997);
- ISN Temporary Resident Identification Card; or,
- ISN Employment Authorization Card.

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two of the following:

- Utility bill (showing address);
- Jurisdictional Voter Registration Card;
- Vehicle Registration Card/Title;

- Paycheck stub with name and address;
- Jurisdictional Public Assistance Card;
- Spouse/Parent affidavit;
- Canceled check or bank statement, or,
- Mortgage documents.

When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state's central repository. Some examples include: Establish provisions for the agency to manage both manually and electronically captured fingerprints; establish an agency tracking system (applicant log) using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity; establish procedure that documents the type of identification used by the applicant; establish procedures that use specially sealed envelopes, agency specific stamps, etc., for the agency to use when forwarding the applicant's manual fingerprint card; and implement the use of forms.

8.4 Challenge Procedures

The applicant may contact the MSHP-CJISD to obtain information on how to challenge, correct, or update the Missouri criminal history record. If the applicant is challenging the accuracy or completeness of the FBI criminal history record, they should follow procedures set forth at Title 28 Code of Federal Regulations (CFR) 16.34, or contact the reporting agency.

8.5 Applicant Procedures For Obtaining Personal Record

8.5.1 From MSHP-CJISD — To obtain a Missouri background check for personal review, applicants may use the MACHS portal for a name-check, or fingerprint-based check. For a fingerprint-based personal review, the applicant will use 9999 as the registration number.

8.5.2 From The FBI — Applicants needing an FBI background check may request an "Identity History Summary Checks (Rap Sheets) from the FBI by visiting the FBI's website at: www.fbi.gov

SECTION 9: Criminal History

9.1 Generating A Criminal History

CHRI is submitted to the MSHP-CJISD by means of the charge information contained on the criminal fingerprint card or criminal livescan submission by law enforcement and is tracked by means of the Offense Cycle Number (OCN). After fingerprints have been entered and identified through the Automated Fingerprint Identification System (AFIS) and matched to or assigned a State Identification Number (SID), the arrest is entered into criminal history for the individual. Thus, making the fingerprint submission is the most critical element when creating a criminal history record. It is especially important due to criminals providing alias information or committing identity theft. Without the fingerprint submission, criminal history will not be present.

9.1.1 OCN — Offense Cycle Number indicates an arrest and is also referred to as the tracking number of the arrest. Each OCN in a criminal history record represents an arrest. When an individual is arrested and fingerprinted, the OCN is generated from the fingerprint card and is entered into criminal history after the prints are identified through AFIS (Automated Fingerprint Identification System). When a Record of Arrest and Prosecution (RAP) sheet is requested on an individual that has criminal history, each OCN listed on the RAP sheet will indicate a separate arrest. There may be one or more charges present with each OCN. The OCN is crucial to prosecutors and courts when submitting prosecutor action and court disposition to the Central Repository.

9.1.2 SID — State Identification Number is assigned to the first set of fingerprints received on an individual at the Central Repository. A SID number does not indicate that a person has a criminal record. Every person fingerprinted in Missouri, whether for civil purposes, such as employment or licensing, or from a criminal arrest card stemming from an arrest by law enforcement, will have an assigned SID once the fingerprints are processed through AFIS. This SID number for Missouri will accompany the individual throughout their life and will never change.

9.1.3 The Missouri Charge Code *is* the state statute that describes the crime and associated penalties used by criminal justice agencies. The charge code will indicate felony, misdemeanor, infractions, and local ordinance charges and classifies each offense according to the law.

Contributing agencies include law enforcement agencies, prosecutors, courts, Department of Mental Health, and Department of Corrections.

CHRI is defined and has three parts as follows:

- The arresting agency's name and crime class under which the person was arrested. The arrest data submitted includes the mandatory field of name, race, sex, and date of birth. All arrests are accompanied by fingerprints.
- The charge(s) issued by the prosecutor.
- The name of the court that tried the case and the ultimate disposition of the case.

CHRI and custody information is compiled from information submitted to the MSHP-CJISD from contributing agencies. Although the MSHP-CJISD makes reasonable efforts to ensure all information is submitted as required by law, it is not responsible for omissions from contributing agencies.

CHRI is constantly being updated as new arrests and other information are entered into the system by contributing agencies. Certain statutes allow for the suppression or deletion of records, such as expungements, and when this occurs, this information is not retained in the system.

9.1.4 Criminal History Records — Missouri records based on fingerprint submission and legislative authority include all criminal history data contained within the systems of the MSHP-CJISD. The data includes all arrests, filed and not filed charges, charges that have been nolle prossed, dismissed charges, or a found not guilty in a court of law determination, and will include any suspended imposition of sentence (SIS) during and after the probationary period.

Open records include convictions and plea of guilt, arrest charges within the first 30 days, pending charges, and suspended imposition of sentence (SIS) while on probation.

Closed records include all open records in addition to those accused and found not guilty, charges that were nolle prossed or dismissed, an SIS after probation is complete, and arrests after 30 days when no charges have been filed.

FBI criminal history obtained through the MSHP-CJISD contains arrest data from all contributing states. Records include those retained within the systems of the FBI and those held by NFF states.

Once fingerprints and arrest information are received at the MSHP-CJISD, the record information is always retained with the exception of expungement.

9.2 Record Of Arrest & Prosecution (RAP) Sheet

A RAP sheet is a listing of certain information taken from fingerprint submissions retained by the MSHP-CJISD and the FBI. If the fingerprints are related to an arrest, the RAP sheet will include the name of the agency that submitted the fingerprints to MSHP-CJISD or the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest, if known. All arrest data included in a RAP sheet is obtained from fingerprint submissions, disposition reports, and other information submitted by agencies having criminal justice responsibilities.

A RAP sheet may be generated when fingerprint submissions are received by the MSHP-CJISD and FBI. Applicant fingerprint submissions by agencies having authority to receive full CHRI will receive Missouri open and closed information, as well as, any records maintained by the FBI.

When a RAP sheet is requested for an individual that has criminal history, each OCN listed on the RAP sheet will indicate a separate arrest. There may be one or more charges present with each OCN. A RAP sheet is considered complete when you have the arrest, prosecution, and court information. Other agencies that submit information to the criminal history record repository will be listed as part of the disposition. Non-criminal justice agencies use background checks for employment, licensing, adoption, citizenship verification, and firearm purchases. In any of these cases, if a disposition is not present on the applicant's record, this could prevent or delay finalization of these proceedings.

9.3 Expungement Of Arrest Records

Information regarding expungement of records is listed in Chapter 610 RSMo.

9.4 National Fingerprint File (NFF)

9.4.1 National Fingerprint File (NFF) States — There are 20 NFF state participants. In 2013, Missouri became the 17th state to be approved for NFF participation by the FBI CJIS Division. For a list of NFF states, please refer to the FBI's website at www.fbi.gov.

9.4.2 Benefits Of Record Control — NFF states control record usage. An NFF participating state is queried directly for its record via III. The III record request identifies the purpose for the request, providing the NFF state the benefit of always knowing when its records are being used and for what purpose.

An NFF state provides its records for all purposes; thus, any request for an NFF state's maintained record when a national fingerprint-based check is conducted, results in the NFF state's repository being queried directly for its CHRI.

An advantage to being an NFF state is the reduction of duplicative record maintenance. Once the decentralization occurs and the NFF state fully maintains their criminal history records, there is no need to duplicate records at the federal level. Missouri is not required to forward expungement notices and disposition information to the FBI. Once a record is initially indexed at the FBI, subsequent arrest submissions are not required.

SECTION 10: State Agency, Board, Or Commission

10.1 Access & Use — Based On Public Law 92-544 & State Statute

Pursuant to Public Law 92-544, the FBI may exchange CHRI with officials of state and local governments for purposes of licensing and employment if authorized by a state statute. The purpose and use of the CHRI must be specifically stated in state statute, and must indicate that the request is fingerprint-based and includes access to national criminal history. The legislative authorization must, expressly or by implication, authorize the use of the FBI records for screening the applicant.

Most state agencies qualify for access to fingerprint-based CHRI through the Revised Statutes of Missouri (RSMo). Some state agencies have agency-specific laws that require state and FBI background checks for licensing or employment. The statutes that are relative to their agency are specific to what they can request and obtain based on a specific purpose.

10.2 Requesting Access

To obtain an ORI, the agency representative should contact the MSHP-CJISD to begin the process. Whether it's a new ORI request, or a modification to an existing ORI authorization, the review process can take several months.

To request a new ORI or to modify an existing ORI, agencies must:

1. Submit a letter of request to the MSHP-CJISD;
2. Submit a copy of the authorizing statute.

The MSHP-CJISD reviews all requests for noncriminal justice ORI use. If deemed appropriate, and meets the Public Law 92-544 criteria, the MSHP-CJISD forwards the request to the FBI's Criminal Justice Information Law Unit (CJILU) for review and approval.

Upon approval and prior to the use of a new ORI, the agency will be required to submit several forms. For example, required forms include:

1. NCJ User Agreement
2. Local Agency Security Officer form

In addition, the agency will have the ability to enroll in state and national Rap Back programs, select electronic access to the fingerprint results through the MACHS portal, and participate in MACHS Record Retention. Training is provided with every new ORI access.

SECTION 11: Missouri VECHS Agencies

11.1 Access to CHRI — Based on Federal Legislation & Missouri VECHS Program Procedures

In 2006, the FBI notified the MSHP-CJISD that the dissemination of an individual's CHRI to a nongovernmental entity (NGE) with the individual's consent and at his/her direction is not legally objectionable under federal law.

The safety and well-being of children and other vulnerable individuals is a national priority. The National Child Protection Act, as amended by the Volunteers for Children Act, encourages states to authorize fingerprint-based national CHRI background checks of individuals having access to children and other vulnerable people, by enacting legislation under Public Law (Pub.L.) 92-544. The NCPA/VCA also authorizes entities in states without specific Pub. L. 92-544 legislation to obtain national CHRI checks. (Title 42 U.S.C. Section 5119a)

The success of this national initiative of child protection is dependent on the cooperation by the states in the implementation of the NCPA/VCA and other federal or state legislation. (Refer to Prosecutorial Remedies and Other Tools to End the Exploitation of Children Total Act of 2003 and the Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248.) Many states have established programs for conducting criminal history record background checks on individuals who work with children, the elderly, or the disabled. Prior to the MSHP-CJISD establishing the Missouri VECHS (Volunteer and Employee Criminal History Service) program, a VECHS program was developed by the Florida Department of Law Enforcement. Florida's VECHS program used the basic framework of the NCPA/VCA with the added feature of dissemination of an individual's criminal history record to nongovernmental entities at the applicant's request. By establishing strict controls on the access and use of CHRI by entities enrolled in the VECHS program, the Florida Department of Law Enforcement had created a program that facilitates the performance of criminal history record checks on thousands of individuals who work with children, the elderly, and individuals with disabilities.

As a result of the success of the Florida VECHS program, the Compact Council requested the FBI to provide advice on the dissemination under the NCPA/VCA of an individual's CHRI to a NGE with the individual's consent. The FBI has no legal objection to the dissemination of CHRI at the consent of the individual, as the practice does not conflict with federal law. (Title 5 USC 552a (d) (1) and (t) (1).) The FBI advised that other states planning to establish CHRI background check programs, that include the dissemination of CHRI to NGEs, must incorporate the following provisions:

- The state shall establish procedures for program participation by nongovernmental entities which serve children, elderly, or individuals with disabilities.
- The NGE must execute a user agreement that sets out the terms under which the criminal history record checks may be performed. This includes the security requirements for protection of the CHRI and the procedures for challenging the accuracy and completeness of the CHRI as entitled by the NCPA/VCA and 28 Code of Federal Regulation 50.12.
- The NGE shall obtain an executed consent form (waiver) from every employee or volunteer subjected to the criminal history record check. The NGE shall retain the original waiver for audit purposes by the MSHP-CJISD. The terms of the waiver must include an acknowledgement that the entity will perform an FBI criminal history records check and that the state is specifically authorized to disseminate the resulting CHRI, if any, to the NGE. The waiver may further authorize the NGE to provide the CHRI to another authorized NGE. The NGE must

maintain a record of any secondary dissemination.

The MSHP's VECHS program was developed in 2008 to provide agencies or qualified entities that provide care or care placement services to children, the elderly, or individuals with disabilities access to Missouri open and closed criminal history records and FBI CHRI with fingerprint submission.

11.1.1 The term "care" means the provision of care, treatment, education, training, instruction, supervision, or recreation to children, the elderly, or individuals with disabilities. (NCPA/VCA)

11.1.2 The term "qualified entity", pursuant to 43.539 RSMo**,** is a person, business, or organization that provides care, care placement, or educational services for children, the elderly, or persons with disabilities as patients or residents, including a business or organization that licenses or certifies others to provide care or care placement services.

The term "qualified entity" is defined in 34 U.S.C. section 40104(10) as: "a business or organization, whether public, private, for-profit, not-for-profit, or voluntary, that provides care or care placement services, including a business or organization that licenses or certifies others to provide care or care placement services."

11.1.3 The term "provider" was replaced with **the term "covered individual,"** pursuant to the Child Protection Improvements Act (CPIA), Public Law (Pub.L.) 115-141, enacted March 23, 2018 and amended the National Child Protection Act/Volunteers for Children Act (NCPA/VCA). The definition of "covered individual" now broadens the category of individuals that a qualified entity may background under the NCPA/VCA to include both individuals that have unsupervised and supervised access to children, the elderly, or individuals with disabilities.

The term "covered individual" is defined in 34 U.S.C. section 40104(9) as: "An individual - (A) who has, seeks to have, or may have access to children, the elderly, or individuals with disabilities, served by a qualified entity; and (B) who -- (i) is employed by or volunteers with, or seeks to be employed by or volunteer with, a qualified entity; or (ii) owns or operates, or seeks to own or operate, a qualified entity."

11.1.4 The term "person" refers to child, elderly, or individuals with disabilities.

The qualified entity may choose to deny the provider unsupervised access to a person to whom the qualified entity provides care.

The VECHS program requires the completion of an application and user agreement and is authorized pursuant to the National Child Protection Act, as amended by Volunteers for Children Act (NCPA/VCA); and the Adam Walsh Child Protection Act (Adam Walsh Act), Section 153 Schools Safe Act (Schools Safely Acquiring Faculty Excellence Act of 2006).

11.1.5 Access for Missouri VECHS. As the authorized recipient for CHRI obtained through the VECHS program, the MSHP-CJISD allows VECHS approved agencies to use ORI's assigned to the MSHP-CJISD to request fingerprint-based state and national CHRI. Dissemination from the MSHP-CJISD to VECHS agencies is authorized through the use of the waiver form and user agreement.

Program approval is based on the specific federal acts that apply to the agency. Although the primary legislation for the VECHS program is the NCPA/VCA, and further amended by the Child Protection Improvements Act of 2017; private elementary and secondary schools wanting to background check employees and volunteers would qualify under the Adam Walsh Act. (Title 42 USC Section 12645g, as referenced in Section 189D (Public Law 111-13)

Since the VECHS program is pursuant to federal law, all VECHS agencies are required to use a Waiver Agreement and Statement form. The Waiver Agreement and Statement adheres to the FBI requirement of Title 28, 16.30-34 and is auditable. Each agency must provide the waiver to the applicant prior to requesting the applicant be fingerprinted. The waiver gives the agency permission from the applicant to obtain their FBI criminal history record, if any, from the MSHP-CJISD. Each VECHS entity is required to produce the waivers during the audit review. Failure to produce waivers during audit will result in a noncompliance assessment.

With agency approval, the MSHP-CJISD allows the agency to use an ORI with an assigned OCA for fingerprint submission and receipt of state and FBI criminal history records. The OCA number is a unique nine-digit number assigned to each agency and identifies the agency by county. Because there are multiple agencies enrolled in VECHS and using the same ORIs, the OCA number is required for tracking and dissemination purposes. All dissemination of criminal history records from the MSHP-CJISD to the VECHS agency is tracked by the ORI and OCA and is used for auditing purposes.

In addition to the assigned ORI and OCA, each agency is also assigned a four-digit MACHS fingerprint registration number to use for electronic fingerprint submission. Both ink fingerprint cards and electronic submission are acceptable.

11.2 Steps To Apply For Missouri VECHS Enrollment

11.2.1 VECHS Enrollment Qualification Process:

1. Is the agency, school, business, or organization exclusively providing direct care or services to children, the elderly, or individuals with disabilities?
2. Is the agency a lawful Missouri business, licensed in Missouri, with a physical operating address in Missouri?
3. Is the agency on file with the Missouri Secretary of State and with a Missouri registered agent?
4. Complete a Missouri VECHS Application (SHP-980).
5. Mail the completed application and the Missouri business license to: Missouri State Highway Patrol, CJIS Division - VECHS Program, P.O. Box 9500, Jefferson City, Missouri 65102-9500.

An interview will be conducted with the point of contact listed on the VECHS application. If the initial interview deems the agency eligible, MSHP-CJISD will proceed with the approval process. Training on criminal history and access will be provided to the agency once the approval process is finalized.

Information about the Missouri VECHS program is available on the Patrol's website at: https://apps.mshp.dps.mo.gov/MSHPWeb/PatrolDivisions/CRID/movechsIndex.html

For questions about the Missouri VECHS program or status of an application, contact MSHP-CJISD at 573-526-6153, extension 5098.

NOTE: Temporary employment agencies, job placement agencies, or personnel staffing agencies do not qualify for Missouri VECHS Program enrollment.

Missouri enrolled VECHS agencies with affiliations to other agencies located outside of Missouri, such as corporate offices, are prohibited from disseminating criminal history to such agency/office. All eligibility reviews and determinations based on the CHRI received through the Missouri VECHS program must be made by the Missouri agency. Dissemination of CHRI outside of Missouri is strictly prohibited. Dissemination to unauthorized entities may result in immediate deactivation.

The MSHP-CJISD is the administrator of the Missouri VECHS program. As the program administrator and ORI designated agency, the MSHP-CJISD has the sole authority to grant or deny Missouri VECHS Program participation.

SECTION 12: Court Access To Criminal History — Civil Functions

12.1 Access & Use

Courts, like law enforcement agencies, have dual roles regarding access and use of CHRI since they are a criminal justice entity and also a noncriminal justice entity when acting in the role of civil or noncriminal justice court functions. This section specifically addresses access to criminal history, with fingerprint submission, for purposes other than criminal justice administration.

For noncriminal justice access to CHRI, courts may apply for a noncriminal justice ORI. The noncriminal justice ORI may be used for eligibility or fitness determinations prior to granting access to minors, the incapacitated, the elderly, or individuals with disabilities. The authority for a court to request and obtain CHRI is pursuant to sections 43.548, 210.160, and 453.070 and includes the following category of persons:

- Prospective Adoptive Parents
- Guardian ad litems
- Conservators
- Court Appointed Special Advocates (CASA)
- Personal Representatives

With an ORI for noncriminal justice purposes, a court has the authority to request fingerprint-based CHRI from the state and FBI for the above purposes.

Although the court is a criminal justice agency and has access to CHRI relating to criminal justice functions, courts are not authorized to request or obtain CHRI from law enforcement agencies with direct terminal access through MULES/NCIC for noncriminal justice purposes. Law enforcement agencies are advised should they receive a request from the court for CHRI for a noncriminal justice purpose, the court should be referred to the MSHP-CJISD for assistance with obtaining a noncriminal justice ORI.

SECTION 13: City/County Government — Access To CHRI

13.1 Authority & Use

Municipal and county government access to CHRI is authorized pursuant to Section 43.535 RSMo By local or county ordinance, background checks based on fingerprints of applicants or licensees in specified occupations for the purpose of receiving CHRI is authorized by local or county officials.

- Specific occupations or categories of persons must be in detail. For example:
- applicants applying for vehicles for hire;
- taxicab license;
- city or county employment;
- volunteers with the city/county government or parks and recreation governed by the city or county;
- security guards that are armed and unarmed;
- liquor licenses;
- solicitors; and
- peddler licenses, etc.

13.2 Procedure For Requesting CHRI

1. The city or county government must enact an ordinance that authorizes state and national fingerprint-based criminal history on applicants in specific occupations or categories of persons.
2. Once the ordinance has been approved, the city or county government will send a letter of request for an ORI and a copy of the approved ordinance to the MSHP-CJISD. (See Appendix E, Forms for sample letter.)
3. The MSHP-CJISD will review the documents.
4. The MSHP-CJISD will send a letter of request and the ordinance copy to the FBI for review and ORI approval.
5. The FBI will either approve or disapprove the ORI request and will notify the MSHP-CJISD.
6. If approved by the FBI, an ORI is assigned and approval notification is sent to the MSHP-CJISD.
7. The MSHP-CJISD notifies the city/county government and provides instructions for use.
8. The city or county government will need to decide what fingerprint method(s) they want to use.

In addition to the fingerprint instructions outlined in Section 8, a city or county government may request their local law enforcement agency to assist with fingerprint submission. If the law enforcement agency has a livescan device and is willing to take the fingerprints and transmit to the MSHP-CJISD, the following is required:

1. The ORI must be added to the law enforcement agency livescan device. All transmissions must indicate the ORI for the city/county government.
2. An "Authorization To Invoice" must be completed by the city/county government. This form will enable the MSHP-CJISD to bill for the electronic fingerprint submissions.
3. For electronic fingerprint submission by a law enforcement agency, the agency must ensure the following:
   - The ORI assigned to the city/county government is used.
   - The reason fingerprinted field must indicate Section 43.535 RSMo
   - The record type must be "X" (state and FBI fees apply).

13.3 Suggested Language — City/County Ordinance

[¶ Enter Ordinance Number]

This ordinance is enacted pursuant to Section 43.535 RSMo, to regulate the issuance of licenses for [*list occupations, i.e. liquor licenses, solicitors/peddlers, etc.*] within the [*enter name of city or county*] and/or employment with [*enter name of city or county government*].

An [*applicant, employee, prospective employee, or volunteer*] seeking to engage in [list occupation(s)] shall submit his/her fingerprints to the Missouri State Highway Patrol Criminal Justice Information Services Division, along with appropriate fees. The Missouri State Highway Patrol CJIS Division will compare the subject's fingerprints against its criminal file and, if necessary, submit the fingerprints to the Federal Bureau of Investigation for a comparison with national criminal history records. The results of the Federal Bureau of Investigation check will be returned to the Missouri State Highway Patrol CJIS Division, which will disseminate the state and national results to [*enter name of city or county government*].

The [enter name of city/county government] shall render a fitness determination based upon the results of the criminal background check. In rendering a fitness determination, the [*enter name of city/county government*] will decide whether the subject of record has been convicted of or is under pending indictment for (a) a crime which bears upon his/her ability or fitness to serve in that capacity; (b) any felony or a misdemeanor which involved force or threat of force, controlled substances, or was a sex-related offense; or (c) enumerated disqualifiers.

The subject of record may request and receive a copy of his/her CHRI from the [*enter name of city/county government*]. Should the subject of record seek to amend or correct his/her record, he/she must contact the Missouri State Highway Patrol CJIS Division for a Missouri state record pursuant to Section 43.535 RSMo, and the Federal Bureau of Investigation for records from other state jurisdictions maintained in its file pursuant to Title 28, CFR 16.30-34.

13.4 Sample Letter To Request An ORI

Address letter of request to:

Date

Captain Gara N. Howard
Missouri State Highway Patrol
1510 E. Elm Street
P. O. Box 9500
Jefferson City, MO 65102-9500

Dear Captain Howard:

The [enter name of city or county government] would like to formally request an Originating Agency Identifier for use in submitting applicant fingerprints for receipt of state and national CHRI pursuant to our Ordinance No. [enter Ordinance #].

It is our understanding with the passage of this ordinance we have met the Public Law 92-544 criteria and Section 43.535 RSMo, to conduct background checks on applicants and licensees in specific occupations including [list the occupations that are specified in the ordinance]. A copy of our ordinance is attached for your review.

Thank you for your assistance with this request. Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,
Representative's Name

Submit a copy of the approved ordinance and Letter of Request to the MSHP-CJISD. When the MSHP-CJISD receives the ORI approval, notification will be forwarded to the city/county government, along with fingerprint instructions, billing instructions, and audit requirements.

SECTION 14: DSS Children's Division

14.1 Emergency Child Placement (Section 210.482 RSMo)

14.1.1 Background — The routine placement of children is a civil function (noncriminal justice function) and does not authorize the use of criminal history inquiries via direct terminal access of MULES/NCIC by criminal justice agencies with the exception of emergency placement or exigent circumstances.

In October 2000, the Compact Council authorized and established procedures for obtaining CHRI for the placement of children in emergency situations or when "exigent" circumstances arise. Generally, "exigent circumstances" refers to an emergency, a pressing necessity, or a set of circumstances requiring immediate attention or swift action. In August 2004, Missouri approved the statute allowing for these checks through state and federal databases such as the Missouri criminal history repository and the III.

The III may be obtained when an authorized state agency is considering the placement of a child with neighbors, friends, or relatives due to the immediate unavailability of a parent or legal guardian.

The Compact Council's interpretation of emergency and exigent circumstances during the emergency placement of children holds that there are two legal principles involved:

1. Exigent circumstances — when time is of the essence and the health and safety of the child are involved, and/or
2. The best interest of the child.

The term "exigent circumstances" includes any placement of a child other than routine foster or licensed care situations.

14.2 Process & Procedure

The Department of Social Services Children's Division (DSS-CD) employee or juvenile court officer (JO) may request a name-based criminal history record check through MULES and NCIC to include active orders of protection and warrants from law enforcement. The inquiry QH using purpose code X is based on the applicant's name, date of birth, and social security number and will indicate if there is or is not criminal history indexed in III. Only with the submission of fingerprints is an applicant's identification and criminal history positively identified. When placement is made in response to an emergency child placement and purpose code X inquiry, fingerprint submission is required within 15 calendar days of placement. (Section 210.482 RSMo)

For each MULES/NCIC inquiry, the ORI of the law enforcement agency is used. The purpose code must indicate "X," the reason field must indicate "emergency child placement," and the attention field or requestor must indicate, at a minimum, the "last name of the DSS-CD employee or JO."

The agency that initiates/requests the purpose code X inquiry is responsible to ensure fingerprints are submitted within 15 days in every instance when child placement occurred. An exception to the fingerprint requirement after child placement is when the applicant refuses to submit fingerprints. (Section 210.482.3 RSMo)

14.3 Direct Terminal Access

Juvenile courts/officers that have direct MULES/NCIC terminal access may conduct an inquiry using purpose code X for emergency child placement for their own information or on behalf of a DSS-CD employee. Juvenile courts/officers without direct access to MULES/NCIC will contact their local law enforcement for the inquiry, and should follow the same procedure as the DSS-CD employee.

Steps to take prior to requesting criminal history (using purpose code X) for emergency child placement:

1. Contact your local law enforcement or JO (if the JO has direct terminal access) and ask if they are willing to provide this service to your circuit.
2. Provide a list of the DSS-CD employee names to law enforcement. This will help law enforcement identify persons that are authorized to request/receive criminal history.

14.3.1 Direct Terminal Access Procedure For Juvenile Court/Officer (JO)

- ORI: MO026009T
- Purpose Code: X
- Reason Field: Emergency Child Placement
- Attention/Requestor Field: Last name of requesting individual — this will be the JO name or CD worker name.

14.3.2 Direct Terminal Access Procedures For Law Enforcement

- ORI: Law Enforcement personnel will enter their agency ORI (Criminal Justice ORI).
- Purpose Code: X
- Reason Field: Emergency Child Placement
- Attention/Requestor Field: Last name of requesting individual — this will be the DSS-CD worker name or JO name.

14.4 Dissemination Procedures

Specific details of any hit notification may be provided to the DSS-CD employee from law enforcement or JO in two ways, depending on agency policy:

- Over the phone
- In hard copy (printed)

Prior to providing specific details of any hit notification over the phone, the identification of the requesting person, i.e. DSS-CD employee or JO, must be verified. Therefore, it is recommended that the DSS-CD employees take the appropriate steps to familiarize themselves with their local law enforcement and juvenile court officers. It is also recommended that a list of authorized DSS-CD employee names are provided to the local law enforcement agencies, ensuring that only authorized DSS-CD employees are requesting the inquiry.

The NCIC/MULES inquiry may include:

- Active orders of protection
- Outstanding warrants
- Criminal history records/arrest information housed with the MSHP-CJISD and FBI

Although a verbal statement of all information obtained from the inquiry is authorized, some law enforcement agencies may only choose to provide a "hit" or "no hit" response. In this instance, the DSS-CD employee may request a hard copy of the criminal history. When a printed copy is requested, it should be picked up in a timely manner.

When the results are requested in hard copy form, the DSS-CD employee must adhere to the following:

- Appear in person at the law enforcement agency.
- Produce a current state photo ID and/or DSS identification badge.
- Sign a secondary dissemination log.

Dissemination of the CHRI obtained from the NCIC/MULES inquiry is strictly prohibited outside of the authorized receiving governmental entity as identified in section 210.482 RSMo. The CHRI is not based on fingerprint submission for positive identification and any other use, other than for the original purpose of the request, is unauthorized. Dissemination of NCIC/MULES record information is governed by Title 28 Code of Federal Regulations Part 20.

14.5 Fingerprint Submission Requirement & Procedures

- For each and every emergency child placement request (using a purpose code X inquiry) that resulted in a child placement, fingerprints must be submitted within 15 calendar days after placement.
- Every effort must be taken by DSS-CD employees to ensure fingerprints are submitted to the MSHP-CJISD within the 15 calendar days after placement. Failure to comply will result in noncompliance.
- In the event the child is removed from the home, even if the child was only placed for a limited time, fingerprints are still required.

The only exception to fingerprint submission is when the applicant refuses to submit fingerprints and the child was removed due to the refusal.

Fingerprint submission is the responsibility of the "requesting entity." If the emergency child placement was requested by the DSS-CD employee, DSS-CD is responsible for fingerprint submission. If the emergency child placement was requested by the JO, the JO is responsible for the fingerprint submission. It is recommended that DSS-CD employees and JOs have an agreement in place to ensure the fingerprint submissions are submitted timely.

14.5.1 Fingerprint Submission By DSS-CD

- ORI : MO920360Z
- Reason Fingerprinted (state law): Section 210.482 RSMo
- OCA: DSS CD Circuit number.

The DSS-CD requires that all applicants submit fingerprints using the state contracted electronic vendor. In order to use the vendor, MACHS registration numbers have been assigned to each DSS-CD Circuit and to DSS Central Office. It is the responsibility of the DSS-CD to instruct applicants on fingerprint submission procedures and to ensure the appropriate four-digit registration number is used. (For MACHS and electronic fingerprint submission procedures, refer to Section 8.)

14.5.2 Fingerprint Submission By Juvenile Court/Officer

- ORI: Court ORI, ending in the letter "J"
- Reason Fingerprinted: Section 210.482 RSMo
- OCA: N/A

Dissemination of the fingerprint-based results to the subject of record is authorized. When disseminating to the subject of record, it is recommended that a copy be made of the original results and marked as "copy." When picking up in person, the subject of record must show photo ID and must sign a secondary dissemination log. (Refer to Section 4 for more details on dissemination and destruction policy.)

14.6 Log Scan Report Procedure — DSS-CD

Log scan reports are generated monthly for every county and sent to the circuit managers. The reports show the names of persons queried for criminal history in response to emergency child placement (using purpose code X). Circuit managers and their staff are responsible for ensuring each inquiry was made for an authorized purpose and that fingerprint submission was obtained from each person when child placement occurred.

SECTION 15: Public Housing Authorities

15.1 Authority & Access

Pursuant to the National Housing Act of 1937, Title 42, USC, Section 1437d(q), the (Act), which was amended by the Housing Opportunity Program Extension Act of 1996 Public Law 104-120, and the Quality Housing and Work Responsibility Act of 1998, Public Law 105-276, administrators of Department of Housing and Urban Development (HUD) assisted housing programs (AHPs) are permitted to obtain CHRI of current and prospective tenants receiving benefits under an AHP, for purposes of applicant screening, lease enforcement, and eviction, where applicable. On May 29, 1996, the HUD and the Department of Justice (DOJ) entered in an agreement which sets forth procedures for the access to criminal history data under the act.

The Act, as amended, provides that a participating agency shall establish and implement a system of records management that ensures criminal records are maintained confidentially, not misused or improperly disseminated, and destroyed once the purpose for which the record was requested has been accomplished. The Act also institutes criminal penalties for improper release of information as well as establishes civil liability for negligence.

In accordance with this agreement, state and local law enforcement agencies are allowed access through the NCIC System to the III for the purposes of determining whether a tenant of, or an applicant for, assisted housing may have a criminal history record indexed in the III. Access for this purpose does not entitle the requesting law enforcement agency to obtain the full content of automated records through III.

In order to receive authority for access to criminal history through NCIC System and III, the Public Housing Authority (PHA) must request an Originating Agency Identifier through the FBI. Generally, ORI requests are sent to the MSHP-CJISD prior to being requested from the FBI; however, PHAs are the exception. The ORI assignment request will be made directly to the FBI, and once approved, the FBI notifies the MSHP-CJISD. When the MSHP-CJISD is notified of the ORI, the ORI is added for access to the state and FBI systems and a Noncriminal Justice Agency User Agreement is sent to the Housing Authority for completion and return to the MSHP-CJISD.

All requests for PHA ORI numbers should be sent directly to the FBI at the following address:

Chief, Programs Support Section
Module E3
FBI Complex
1000 Custer Hollow Road
Clarksburg, WV 26306

The request for ORI should include:

- The full name of the PHA;
- The PHA's complete mailing address;
- The county in which the PHA's main office is located;
- The number of fingerprint cards the PHA will initially need;
- The name and telephone number of the PHA contact person;

- The name of the CA or SIB the PHA will utilize to submit its fingerprint cards to the FBI;
- The FBI will assign an ORI number to the PHA and furnish applicant fingerprint cards to the PHA bearing that ORI number. A reorder form will be included with each supply of fingerprint cards so that the PHA can reorder with necessary.

Public Law 104-120 provides that the NCIC, police departments, and other law enforcement agencies shall, upon request, provide information to PHAs regarding the criminal conviction records of adult applicants for, or tenants of, public housing for purposes of applicant screening, lease enforcement, and eviction. The FBI has established Purpose Code H for housing, to be used when requesting a name search (QH) of III under the authority of Public Law 104-120. Purpose Code H is valid only for QH inquiries when those inquiries are made for a PHA. (NCIC Technical and Operational Update, FBI CJIS Division Informational Letter, dated Dec. 6, 1996)

- The inquiry will include:
- Housing Authority ORI
- Inquiry of QH
- Purpose Code of H

The PHAs are assigned an ORI with a Q in the 9th position for use by a cooperating law enforcement agency to run III name checks using a Purpose Code "H." If the III name check reveals no additional information for the name and other identifiers provided by the applicant/tenant, the PHA need not pursue further inquiries. However, if the search results indicate the possible existence of a criminal history record, the law enforcement agency advises the PHA that they must submit fingerprints to obtain the criminal history. The PHA may only share CHRI received from fingerprint submissions with the subject of record. (Noncriminal Justice Online Policy Resource Use of FBI CHRI for Noncriminal Justice Purposes 03/26/2014)

15.2 Criminal History Record Inquiry & Fingerprint Submission Process

1. PHA applies for an ORI from the FBI.
2. PHA is assigned an ORI, ending with the letter "Q."
3. PHA contacts their local law enforcement agency and enters into a "non-terminal user agreement" for criminal history inquiries by law enforcement through direct (MULES/NCIC) terminal access.
4. The PHA submits a name check request to the law enforcement agency. The name check request must include the name, date of birth, and social security number of the applicant/resident (if he/she has one).
5. Using the ORI assigned to the PHA, the law enforcement agency will access the III through the NCIC to determine whether an applicant may have a criminal history record.
6. The law enforcement agency is authorized to give a "hit or no hit" notification — a hit notification means that the information given may match a criminal record indexed in the national database. This statement means only that based on the information provided, the record may belong to the applicant/resident, but is inconclusive without a positive fingerprint comparison. The results of an inconclusive name check cannot be used to deny an applicant's admission to housing or as a basis to evict a tenant.
7. For positive hit notifications, the PHA must notify the applicant that fingerprints are needed

in order to verify criminal history and receive the full content of the record, if one does exist.

8. The PHA will give the applicant an Applicant Fingerprint Card (FD-258) which has the Housing Authority ORI pre-printed or written on the card. The "reason fingerprinted" field should indicate "housing." (In some instances, where applicable, law enforcement agencies may use their livescan device for electronic capture of fingerprints. The Housing Authority ORI must be used and an "Authorization to Invoice" form must be on file with MSHP-CJISD prior to electronic transmission.)
9. The applicant will take the fingerprint card to their local law enforcement to be inked and then return the completed fingerprint card to the PHA.
10. The PHA should verify that the fingerprint card is completed in full and then mails the fingerprint card with appropriate fees to the MSHP-CJISD for processing.

The applicant's fingerprints will be compared with criminal fingerprints maintained in FBI files; and, if found to be identical, a copy of the corresponding criminal history record will be provided to the PHA.

The PHA may submit fingerprint cards either directly to the FBI or to the responsible SIB (SIB), providing the SIB has agreed to process the cards. The MSHP-CJISD processes fingerprint cards for state and FBI criminal history responses for PHA in Missouri.

It is important to note that, based on Public Law 104-120, the inquiry information is provided to the PHA only to inform them of the probable existence or nonexistence of a criminal history record. The PHA will use the results of the response as a factor in deciding if a fingerprint-based search of criminal history is needed. Only with the submission of fingerprints can a positive identification be made and a record provided, if such a record exists. Therefore, the result of the inquiry should not be used as the basis for disqualification, lease enforcement, or eviction.

15.3 Non-terminal Agency User Agreements

All PHAs with an ORI must have a non-terminal user agreement with the local law enforcement agency that will perform the name-based queries for them. PHAs that have an approved ORI should contact their local law enforcement agency to establish procedures for requesting inquiries.

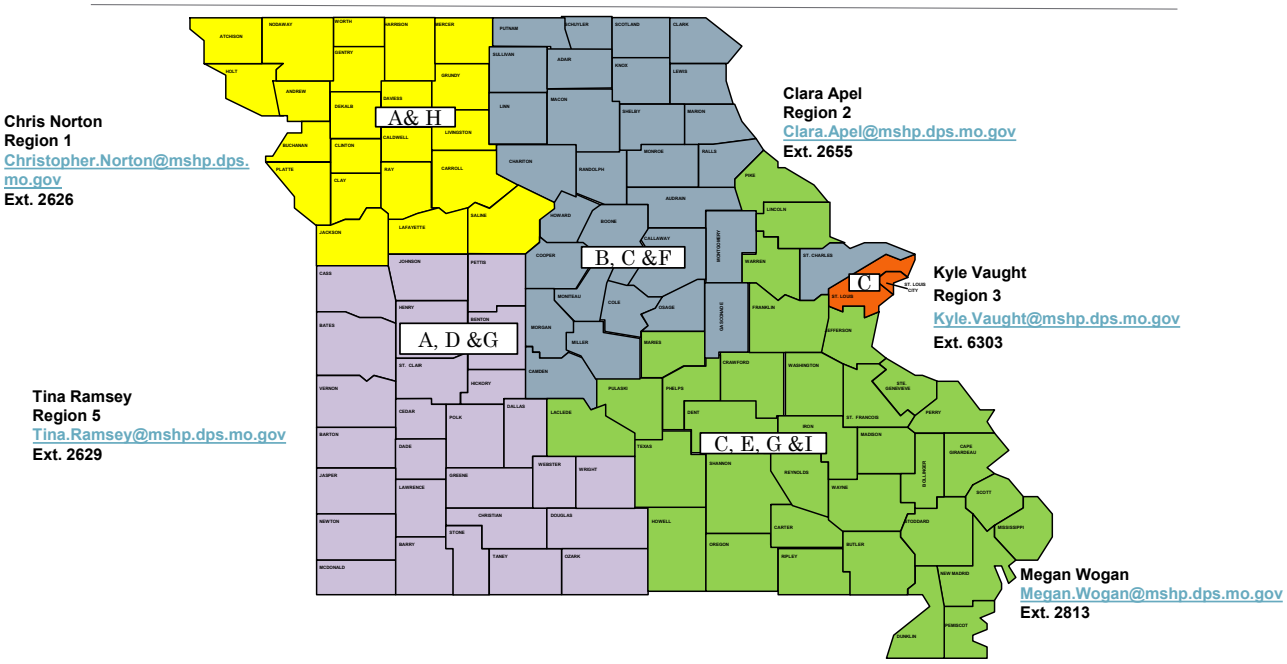
When the non-terminal user agreement is in place between the PHA and the law enforcement agency, inquiries based on an applicant's personal identifiers may be performed through MULES and NCIC.

APPENDIX A — CJIS Trainer/ Auditor Contact Information

The Noncriminal Justice (NCJ) Training and Audit Unit consists of one manager and five individuals who provide statewide training and conduct compliance audits. The official domicile is the Missouri State Highway Patrol, General Headquarters, in Jefferson City, MO.

(573) 526-6153 - Main Number
(978) 244-8842 - FAX
Unit Extension 5098

Noncriminal Justice (NCJ) Training & Auditing Unit



Chris Norton
Region 1
Christopher.Norton@mshp.dps.mo.gov
Ext. 2626

Clara Apel
Region 2
Clara.Apel@mshp.dps.mo.gov
Ext. 2655

Kyle Vaught
Region 3
Kyle.Vaught@mshp.dps.mo.gov
Ext. 6303

Tina Ramsey
Region 5
Tina.Ramsey@mshp.dps.mo.gov
Ext. 2629

Megan Wogan
Megan.Wogan@mshp.dps.mo.gov
Ext. 2813

Main Number (573) 526-6153 -- Unit Extension 5098

MSHP CJIS Division Location — Annex Building

Physical Location
MSHP CJIS Division
Annex Building
1510 E. Elm Street
Jefferson City, MO 65101

Mailing Address
MSHP CJIS Division
P.O. Box 9500
Jefferson City, MO 65102-9500

APPENDIX B: Acronyms

AFIS — Automated Fingerprint Identification System

APB — Advisory Policy Board

AR — Authorized Recipient

CAU — CJIS Audit Unit (FBI)

CFR — Code of Federal Regulations

CHRI — Criminal History Record Information

CJI — Criminal Justice Information

CJIS — Criminal Justice Information Services

CJISD — Criminal Justice Information Services Division

CSA — CJIS Systems Agency

CSO — CJIS Systems Officer

DOJ — Department of Justice

FIPS — Federal Information Processing Standard

FBI — Federal Bureau of Investigation

IAFIS — Integrated Automated Fingerprint Identification System

III — Interstate Identification Index

ISO — Information Security Officer

LASO — Local Agency Security Officer

MACHS — Missouri Automated Criminal History Site

MSHP — Missouri State Highway Patrol

MULES — Missouri Uniform Law Enforcement System

NCIC — National Crime Information Center

NCJA — Noncriminal Justice Agency

NCPA — National Child Protection Act

NGE — Nongovernmental Entity

NICS — National Instant Criminal Background Check System

NFF — National Fingerprint File

OCA — Originating Case Agency

OCN — Offense Cycle Number

ORI — Originating Agency Identifier

PHA — Public Housing Authority

PCR — Policy Compliance Review

PII — Personally Identifiable Information

POC — Point of Contact

RAP — Record of Arrest & Prosecution

RSMo — Revised Statutes of Missouri

SAT — Security Awareness Training

SIB — State Identification Bureau

SID — State Identification Number

TCN — Transaction Control Number

USC — United States Code

VCA — Volunteers for Children Act

VECHS — Volunteer and Employee Criminal History Service

APPENDIX C: Terms & Definitions

These definitions are derived from the CJIS Security Policy, Title 28 CFR Section 20.3, the National Crime Prevention and Privacy Compact Council (Compact), and the Revised Statutes of Missouri.

Access to CHRI/CJI — The physical or logical (electronic) ability, right, or privilege to view, modify, or make use of criminal justice information.

Administration of Criminal Justice — 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. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history information, including fingerprint searches, photographs, and other indicia of identification.

Arrest — An actual restraint of the person of the defendant, or by his or her submission to the custody of the officer, under authority of a warrant or otherwise for a criminal violation which results in the issuance of a summons or the person being booked.

Arrest Report — A record from a law enforcement agency of an arrest and of any detention or confinement incident thereto together with the charge therefore.

Audit — The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A NGE authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Authorized State Agency — A division of state government or an office of state government designated by the statutes of Missouri to issue or renew a license, permit, certification, or registration of authority to a qualified entity.

Background Check — A check of all appropriate information sources to include a state of residency and national tenprint-based (fingerprints) record check.

Care — Refers to the provision of care, treatment, education, training, instruction, supervision, or recreation.

Central Repository — The Missouri State Highway Patrol Criminal Justice Information Services Division, which is responsible for compiling and disseminating complete and accurate criminal history records, and for compiling, maintaining, and disseminating criminal incident and arrest reports and statistics.

Channeler — An FBI approved contractor, who has entered into an agreement with an authorized recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The channeler ensures fingerprint submissions are properly and adequately completed, electron-

ically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to authorized recipients. A channeler is essentially an "expediter" rather than a user of criminal history record check results.

Child — Any person, regardless of physical or mental condition, under 18 years of age.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies' connection to the FBI CJIS systems.

CJIS Systems Officer (CSO) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Confidential Information — Information maintained by the state agency that is exempt from disclosure under the provisions of the Public Records Act or other applicable state or federal laws. The controlling factor for confidential information is dissemination. CHRI is protected by federal legislation.

Contractor — A private business, agency, or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a criminal justice agency or a noncriminal justice agency. Also, a private business approved by the FBI CJIS Division to contract with noncriminal justice agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Criminal History Records — (1) Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, or release; and (2) does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

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

Criminal Justice — Activities relating to the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history records.

Criminal Justice Agency — (1) Courts, and (2) a governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. Inspector General offices (state and federal) are included.

Criminal Justice Information (CJI) — Criminal justice information is the abstract term used to refer to all the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws including, but not limited to, biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for noncriminal justice/civil agencies to perform their mission; including, but not limited to, data used to make hiring decisions.

Criminal Justice Information Services Division (CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, and Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Disposition — Information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

Dissemination — The transmission or distribution of CJI to authorized recipients.

Dissemination Log — Paper or automated log that records the transfer or release of CHRI.

Exigent Circumstances — A sudden unexpected event that results in an apparent risk to the health and safety of an individual that necessitates immediate action on the part of the state to provide protection to that individual.

FBI (Federal Bureau of Investigation) — An agency within the Department of Justice responsible for protecting and defending the United States against terrorist and foreign intelligence threats, upholding

and enforcing the criminal laws of the United States, and providing leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS advisory process comprised of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to FBI CJIS Division programs and makes subsequent recommendations to the director of the FBI.

Final Disposition — Formal conclusion of a criminal proceeding at whatever stage it occurs in the criminal justice system.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assess threats and vulnerabilities, perform risk and control assessments, oversee the governance of security operations, and establish information security training and awareness programs. The ISO usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interstate Identification Index System (III System) — The cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

Local Agency Security Officer (LASO) — The primary information security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with information security audits of hardware and procedures, and keeps the CSA informed as to any information security needs and problems. For noncriminal justice purposes, the LASO serves in the same capacity although FBI CHRI is received based on fingerprints and not through direct terminal access.

Missouri Charge Code — A unique number assigned by the Office of State Courts Administrator to an offense for tracking and grouping offenses.

MULES — Missouri Uniform Law Enforcement System is a statewide-computerized communications system provided by the Patrol designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the state of Missouri.

National Crime Information Center (NCIC) — The computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the attorney general of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC-related information. The NCIC includes, but is not limited to, information in the III System.

National Criminal Record Review — Review of the criminal history records maintained by the Federal Bureau of Investigation.

nolle prossed — A formal notice of abandonment by a plaintiff or prosecutor of all or part of a suit or action.

Noncriminal Justice Agency (NCJA) — A governmental or non-governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Non-Criminal Justice Purposes — The use of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — The National Crime Prevention and Privacy Compact Council Outsourcing Standard provides uniform standards and processes for the interstate and federal-state exchange of criminal history records for noncriminal justice purposes.

Personally Identifiable Information (PII) — Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Positive Identification — A determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III system. Identifications based solely upon a comparison of subject's name or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

Provider — A person who has or may have unsupervised access to children, the elderly, or persons with disabilities, and is employed by or seeks employment with a qualified entity, or volunteers or seeks to volunteer with a qualified entity, or owns or operates a qualified entity.

Qualified Entity — A person, business, or organization, whether public or private, for profit, not for profit, or voluntary, that provides care, placement, or educational services for children, the elderly, or persons with disabilities as patients or residents, including a business or organization that licenses or certifies others to provide care or placement services.

RAP Back — An IAFIS service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI and committed by persons of interest.

Secondary Dissemination — Re-dissemination of FBI CJIS data or records from an authorized agency that has direct access to the data to another authorized agency.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the

paper into long, thin strips, but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

State — Any state of the United States. For the purpose of this CJIS—NCJ Policy Manual, the word state refers specifically to Missouri.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository, or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Offense Cycle Number — A unique number, supplied by or approved by the Missouri State Highway Patrol, on the state criminal fingerprint card. The offense cycle number (OCN) is used to link the identity of a person, through fingerprints, to one or many offenses for which the person is arrested or charged. The OCN will be used to track an offense incident from the date of arrest to the final disposition when the offender exits from the criminal justice system.

Statute — An act of congress or of a state legislature or a provision of the Constitution of the United States or of a state.

User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and NCJA, and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

APPENDIX D: Laws

This section is for reference only and may not be all inclusive of laws that grant access to CHRI.

REVISED STATUTES OF MISSOURI

Chapter 43 — Criminal Records, Central Repository

Section 43.500 RSMo — Definitions.

Section 43.527 RSMo — Payment for records, exceptions.

Section 43.530 RSMo — Fees, method of payment — Criminal Record System Fund, established — fund not to lapse.

Section 43.532 RSMo — Use of records, limitations, — authority of Central Records Repository to retain information — unlawful obtaining of information penalty.

Section 43.535 RSMo — Municipal and county government, MULES criminal record review permitted, fee — fingerprinting, when — confidentiality.

Section 43.539 RSMo — Criminal record review, youth agencies and care of children, elderly, or disabled persons - definitions - Rap Back program, requirements, fingerprints - information to be provided by applicant - confidentiality - notification and forms provided by patrol.

Section 43. 540 RSMo — Criminal records review — definitions — Patrol to conduct review, when, procedures, confidentiality, violations, penalty — Patrol to provide forms.

Section 43.542 RSMo — Approval of National Crime Prevention and Privacy Compact — Execution of Compact.

Section 43.543 RSMo — Certain agencies to submit fingerprints, use of fingerprints for background search — procedures for submission.

Section 43.546 RSMo — Fingerprinting of applicants for background checks permitted by state agencies, boards, and commissions, when — procedures.

Section 43.547 RSMo — Gubernatorial appointees, fingerprint background checks required — procedures.

Section 43.548 RSMo — Care of minors, elderly, or disabled persons, fingerprinting of applicants permitted.

Chapter 67 — Political Subdivisions, Miscellaneous Powers — Regional Taxicab Districts (St. Louis)

Section 67.1818 RSMo — Licensure, taxicab code to include administrative procedures.

Section 67.1819 RSMo — Background checks required, when — payment of fees.

Chapter 168 — Personnel — Teachers & Others

Section 168.071 RSMo — Revocation, suspension, or refusal of certificate or license, grounds, procedure, and appeal.

Section 168.133 RSMo — Criminal background checks required for school personnel, when, procedures — rulemaking authority.

Chapter 192 — Department of Health and Senior Services

Section 192.2495 RSMo — Criminal background checks of employees, required when - persons with criminal history not to be hired, when, penalty - failure to disclose, penalty - improper hiring, penalty - definitions - rules to waive hiring restrictions.

Chapter 210 — Child Protection & Reformation

Section 210.482 RSMo — If the emergency placement of a child in a private home is necessary due to the unexpected absence of the child's parents, legal guardian, or custodial, the juvenile court or children's division ...

Section 210.487 RSMo — When conducting investigations of persons for the purpose of foster parent licensing, the division shall ...

Section 210.903 RSMo — Family care safety registry and access line established, contents.

Chapter 302 — Driver & Commercial Driver Licenses

Section 302.060 RSMo — License not to be issued to whom, exceptions — reinstatement requirements.

Section 302.309 RSMo — Return of license, when — limited driving privilege, when granted, application, when denied — judicial review of denial by director of revenue — rulemaking.

Chapter 313 — Licensed Gaming Activities

Section 313.220 RSMo — Rules and regulations — procedure generally, this chapter — background checks may be required, when.

Section 313.810 RSMo — Applicants contents, fingerprint submissions — investigations, commission may conduct — false information on application, penalty.

Chapter 453 — Adoption & Foster Care

Section 453.070 RSMo — Investigation preconditions for adoptions — contents of investigation report — how conducted — assessments of adoptive parents, contents — waving of investigations, when — fees — preference to foster parents, when.

Chapter 590 — Police Officers Standards & Training (POST)

Section 590.060 RSMo — Minimum standards for training instructors and centers — licensure of instructors — background check required, when.

Chapter 610 — Governmental Bodies and Records

Section 610.120 RSMo — Records to be confidential — accessible to whom, purposes.

Section 610.122 RSMo — Arrest record expunge, requirements.

Section 610.123 RSMo — Procedure to expunge, Missouri Supreme Court to promulgate rules — similar to small claims.

Section 610.126 RSMo — An expungement of an arrest record shall not reflect on the validity of the arrest and shall not be construed to indicate a lack of probable cause for the arrest.

Section 610.130 RSMo — Alcohol-related driving offenses, expunged from records, when— procedures, effect — limitation.

Section 610.140 RSMo — Expungement of certain criminal records, petition, contents, procedure.

Chapter 621 — Administrative Hearing Commission

Section 621.045 RSMo — Commission to conduct hearings, make determinations — boards included — settlement agreements — default decision, when.

FEDERAL CRIMINAL HISTORY-RELATED REPORTING LAWS

According to federal law (Title 28 USC 534), the FBI has authority to collect and exchange CHRI for criminal justice and noncriminal justice purposes. As complex and diverse as the federal government is, there are several governmental actions that dramatically affect the way a federal agency may use the personal information it houses. Since the FBI has the authority to collect and disseminate criminal history information and criminal history information is considered private, the FBI must abide by federal laws, i.e. the Privacy Act of 1974 and the Freedom of Information Act.

TITLE 5

Title 5, U.S.C 552, as amended by Public Law 104-231, 110 Stat. 3048, Freedom of Information Act — The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to the U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government, not the public, to substantiate why information may not be released. FOIA allows an individual to consent to the disclosure of information about the individual from federal agencies to third parties. This includes access to an individual's criminal history record maintained by the FBI. There are no restrictions regarding the purpose of a FOIA request and, therefore, an individual could make such a request for his/her FBI criminal record and either provide it to an employer or specify that the record be sent directly to an employer. FBI maintains that the federal Privacy Act of 1974 protects CHRI and its disclosure is prohibited without consent from the individual who is the subject of the information or a state statutory exception that authorizes disclosure. (Title 5 USC 552a)

Title 5 U.S.C. Section 552a, **Privacy Act of 1974** — The Privacy Act reaffirmed an earlier law (Public Law 92-544), in that it specified, "no governmental agency shall disclose any records to any person or agency unless prior written consent is received from the individual or it is used by the agency to perform the duties of the agency." With the Privacy Act of 1974, government agencies may release certain information; however, they must track the dissemination of each record including the time, date, purpose, and to whom the information was disclosed. The information may not be disclosed except for government use or unless it is authorized by applicable law or state statute.

TITLE 42

Title 42 U.S.C. 14616, Part 907 — This rule establishes policies and procedures to ensure that use of the III System for noncriminal justice purposes complies with the National Crime Prevention and Privacy Compact Council (Compact Council) and with rules, standards, and procedures established by the Compact Council regarding application and response procedures, record dissemination and use, response times, data quality, system security, accuracy, privacy protection, and other aspects of III System operation for noncriminal justice purposes. This rule is established pursuant to Article VI of the Compact.

Title 42 U.S.C. 14616, Article V (b) — Each request for a criminal history record check utilizing the national indices made under any approved state statute shall be submitted through the state's criminal history record repository. A state criminal history record repository shall process an interstate request for noncriminal justice purposes through the national indices only if such request is transmitted through another state criminal history record repository or the FBI.

Title 42 U.S.C 14616, Article V (d). Fees. (1) — A state criminal history record repository or the FBI may charge a fee, in accordance with applicable law, for handling a request involving fingerprint processing for noncriminal justice purposes.

PUBLIC LAWS

Public Law 92-544, **Violent Crime Control and Law Enforcement Act** — This act, passed in 1972 by the U.S. congress, is an appropriations statute that provides funding to the FBI for acquiring, collecting, classifying, preserving, and exchanging identification records with duly authorized officials of the federal government, states, cities, and other institutions for the purpose of licensing and employment if authorized by state statute. The law, however, did not provide guidelines for obtaining federal criminal background checks. The authorization to disseminate criminal history information for the purposes of licensing and employment was restricted with a stipulation requiring a state statute authorizing the use of the information and approval by the U.S. attorney general.

Public Law 103-159, The Brady Act, The National Criminal Instant Background Check System (NICS) — Established as part of the Brady Handgun Violence Prevention Act of 1993, it is a national system that cross-references NCIC, III, and the NICS index to search for individuals that are, by federal law, prohibited from receiving firearms.

Public Law 103-209 — The National Child Protection Act (NCPA) allows access to FBI criminal history for qualified entities providing care to children, the elderly, or individuals with disabilities.

Public Law 104-120, Title 42 — The Housing Opportunity Program Extension Act of 1996, followed by the Quality Housing and Work Responsibility Act of 1998 (Public Law 105-276), allows the administrators and officials of the U.S. Department of Housing and Urban Development (HUD) authority to obtain criminal history records from the FBI for the purpose of applicant screening, lease enforcement, and eviction.

Public Law 105-251, **Volunteers for Children Act (VCA)** — This act amended the NCPA/VCA of 1993, and further expanded the ability to receive criminal history to protect children, the elderly, and individuals with disabilities.

Public Law 108-458, **Section 6402 of the Intelligence Reform and Terrorism Prevention Act of 2004, included the Private Security Officer Employment Authorization Act** — Authorizes a fingerprint-based criminal history check of state and national criminal history records to screen prospective and current private security officers.

Public Law 109-248, **Adam Walsh Child Protection & Safety Act,** ***Sections 151 and 153, Adam Walsh Child Protection and Safety Act of 2006*** — Requires the attorney general to ensure access to FBI CHRI by (1) governmental social service agencies with child protection responsibilities, (2) child welfare agencies, and (3) public and private elementary and secondary schools and state and local educational agencies.

Section 151, Public Law 109-248, Adam Walsh Child Protection & Safety Act — This act provides that access by governmental social service agencies with child protection responsibilities is to be used only in investigating or responding to reports of child abuse, neglect, or exploitation. An ORI with an "F" in the ninth position is required and purpose code C must be used when making III queries.

Section 153, Public Law 109-248, Adam Walsh Child Protection & Safety Act, Schools SAFE Act — "Schools Safely Acquiring Faculty Excellence Act of 2006" — This act allows for fingerprint-based checks of national crime information databases (as defined in 28 U.S.C. Section 534) by private or public elementary or secondary schools, or local or state educational agencies.

Public Law 111-13, The Edward M. Kennedy Serve America Act — This act requires volunteers working with vulnerable citizens be background checked through FBI.

Public Law 113-186, Child Care and Development Block Grant Act of 2014 — To allow each State maximum flexibility in developing child care programs and policies that best suit the needs of children and parents within that State, requires a State that receives funds...shall have in effect...requirements, policies, and procedures to require and conduct criminal background checks for child care staff members...licensing, regulation and registration requirements.

TITLE 28

28 United States Code (USC) 534 — This code pertains to acquisition, preservation, and exchange of identification records and information, appointment of officials.

Title 28, Code of Federal Regulations (CFR) Part 901 — This code outlines fingerprint submission requirements. The Compact Council provides that "subject's fingerprints or other approved forms of positive identification shall be submitted with all requests for criminal history record checks for noncriminal justice purposes." (Title 42 USC 14616 Article V (a). The Compact Council recognizes the extreme reliability of fingerprint-based identifications and requires that fingerprints be submitted contemporaneously with search requests whenever feasible. (Exception to this rule is exigent circumstances, 28 CFR 901.2(a) (2), which is also approved in Section 210.482 RSMo)

Title 28, CFR 901.1 — This code applies to the required submission of fingerprints, along with requests for III records, by agencies authorized to access and receive criminal history records under Public Law 92-544. It establishes protocols and procedures applicable to the III and its use for noncriminal justice purposes.

Title 28, CFR 901.2 — (a) Article V of the Compact Council requires the submission of fingerprints or other approved forms of positive identification with requests for criminal history record checks for noncriminal justice purposes. The requirement for the submission of fingerprints may be satisfied in two ways: (1) The fingerprints should be submitted contemporaneously with the request for criminal history information, or (2) For purposes approved by the Compact Council, a delayed submission of fingerprints may be permissible under exigent circumstances. (Section 210.482 RSMo)

Title 28 CFR Part 901.4 — This code states that audits of authorized state agencies that access the III System shall be conducted by the state's Compact Officer ... such audits shall be conducted to verify adherence to the provisions of Part 901 and the FBI's CJIS Security Policy.

Title 28, CFR Part 907 — This code covers Compact Council Procedures for Compliant Conduct and Responsible Use of the III System for Noncriminal Justice Purposes.

Title 28 CFR, Chapter I, Part 20 — This code provides information regarding the NCIC (NCIC), and preparation and submission of CHRI to the FBI.

Title 28 CFR 20.33 — This code restricts the use of CHRI. Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

Title 28 CFR 50.12 — This code addresses the exchange of FBI identification records. Records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.
Note: Federal law sets forth the minimum standards regarding access and use of CHRI. The states may make laws more restrictive, but not less restrictive. (FBI CJIS Audit Aug. 2009)

Bibliography

Criminal Justice Information Services (CJIS) Security Policy, U.S. Department of Justice, Federal Bureau of Investigation CJIS Division, CJISD-ITS-DOC-08140-5.9, 2020.

Missouri Uniform Law Enforcement System (MULES) Policy and Procedures Manual, Missouri State Highway Patrol CJIS Division, 2014.

NCIC Operating Manual, U.S. Department of Justice, Federal Bureau of Investigation, 2015.

Standard Operating Procedures, Missouri State Highway Patrol CJIS Division, 2015.

Questions or comments regarding the information contained within this document may be directed to:

Missouri State Highway Patrol
Criminal Justice Information Services Division (CJISD) – NCJ Training & Audit Unit
1510 E. Elm Street
P. O. Box 9500
Jefferson City, MO 65102-9500
Telephone Number: (573) 526-6153 ext. 5098
Fax Number: (978) 244-8842