MACHS II Training

For

Missouri Public School Personnel

Presented by the CJIS Division

Introduction

- Today's training is being presented as a webinar with the assistance of the Department of Elementary and Secondary Education (DESE).
- The purpose of training is to provide guidance to school district personnel in regards to the use of the Missouri Automated Criminal History Site (MACHS) and to ensure compliance with the CJIS Security Policy and state and federal laws governing access.
- Training is mandatory for each district prior to access.

Training consists of 3 parts:

Part 1: Access of Criminal History Record Information (CHRI) which includes an overview of:

a) Laws governing access and use
b) Applicant Privacy Rights
c) Security, Retention, Destruction and Dissemination

Part 2: Security Awareness Training

Part 3: MACHS Electronic System Demo

Part 1: Access of Criminal History Record Information (CHRI)

Who has access and why?

- Criminal justice agencies for the administration of criminal justice, which include:
  - Law enforcement
  - Courts
  - Prosecutors
- Public or private agencies, for employment, licensing or other authorized benefit, based on state/federal law, such as:
  - Social Services
  - DESE/school districts
  - City/County Municipalities
  - VECHS agencies

What is Access?

- Access means to view or make use of CHRI obtained from the III System (Interstate Identification Index)
- For your agency to have access, you must have an approved Originating Agency Identifier (ORI) and statutory authority (state or federal law).
- You must have a signed User Agreement
- Access requires fingerprints.

User Agreement Overview

- Pursuant to the CJIS Security Policy, an agency must enter into a written agreement in order to access fingerprint-based criminal history records.
- The user agreement will:
  - Specify the statute,
  - Identify the specific type of applicants
- It outlines the responsibilities of both the Authorized Recipient (AR) and the Patrol.

Access is governed by

- Public Law 92-544
  - Authorizes the FBI to exchange records with state and local governments for licensing and employment purposes. (Oct. 1972)
- The National Crime Prevention and Privacy Compact Act (Compact Council)
  - Establishes an infrastructure by which states can exchange criminal records for *noncriminal justice purposes* according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information.
  - In 2003, through legislative enactment of Section, 43.542 RSMO., Missouri approved and adopted the compact to facilitate the exchange of criminal history information for noncriminal justice purposes.

Agency Privacy Requirements

AGENCY PRIVACY REQUIREMENTS FOR NONCRIMINAL JUSTICE APPLICANTS

Authorized governmental and non-governmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as a job or license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notice and other information and that the results of the check are handled in a manner that protects the applicant's privacy.

- Officials must provide to the applicant written notice[1] that his/her fingerprints will be used to check the criminal history records of the FBI.
- Officials using the FBI criminal history record (if one exists) to make a determination of the applicant's suitability for the job, license, or other benefit must provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.
- Officials must advise the applicant that procedures for obtaining a change, correction, or updating of an FBI criminal history record are set forth at Title 28, Code of Federal Regulations (CFR), Section 16.34.
- Officials should not deny the job, license, or other benefit based on information in the criminal history record until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so.
- Officials must use the criminal history record solely for the purpose requested and cannot disseminate the record outside the receiving department, related agency, or other authorized entity.[2]

The FBI has no objection to officials providing a copy of the applicant's FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at 28 CFR 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant's suitability.

Each agency should establish and document the process/procedures it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct or complete the record, and any applicant appeal process that is afforded the applicant. Such documentation will assist State and/or FBI auditors during periodic compliance reviews on use of criminal history records for noncriminal justice purposes.

Required for all agencies requesting fingerprint-based national records for noncriminal justice purposes.

What type of information are you obtaining?

- The type of information returned on a fingerprint-based background check will depend on the purpose and authority.
- Certain qualified entities will be entitled to Missouri open and closed record information and FBI data, while other agencies will only be entitled to Missouri open record information.
  - With an ORI and an approved state or federal law, your agency will have access to Missouri open/closed and FBI records.

What does the record include?

- Criminal history record information has three parts:
  - 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.

For authorized agencies, CHRI will include:

- All arrests
- File and not filed charges
- Charges that have been nolle prossed, dismissed and found not guilty in a court of law, and
- Any suspended imposition of sentence (SIS) during and after the probationary period.
  - FBI CHRI contains arrest data from all contributing states. Records include those retained within the systems of the FBI and those held by NFF states.

Access Levels for MACHS

- As the Authorized Recipient/designee of the ORI, DESE personnel are the account ORI Administrators. ORI Administrators have full access including all OCAs.
- ORI Read Only – CHRI access.
- OCA Administrator - is similar to ORI Administrator access but is only at the OCA level.
- OCA Read Only – CHRI access. This is the level designated for school districts.

CHRI Security and Retention

- Your agency will need to ensure that the CHRI is kept secure and access is given only to those who have the need to view it in the official capacity of their duties.
- With the receipt of the CHRI through MACHS, you need to have a policy regarding security/retention.
  - Do you intend to: a) print and keep in hard copy, b) save in electronic form, or c) leave on our secure website and it will delete after 90 days?
- CHRI does not need to be retained for audit purposes. It may be destroyed when it has served the purpose for which it was requested.

CHRI Maintenance and Destruction

- If your agency is keeping the CHRI, you must ensure it is kept in a secure area, free from public or unauthorized access.
  - A secure area is defined by the FBI as an area or room(s) within a facility with both the physical and personnel security controls sufficient to protect the information.
- If your agency is destroying CHRI, ensure it is destroyed in an acceptable manner.
  - Shredded or incinerated. If contracted service, destruction must be supervised.
  - For electronic destruction, give to your IT staff.

Authorized Dissemination

- Subject of Record
  - As a best business practice, when disseminating to the applicant, ask the applicant to pick up the results in person and sign a secondary dissemination log.
  - You are <u>not</u> required to disseminate.
  - If your agency policy permits dissemination, supplying a copy to the applicant may assist in correcting his/her record.

Dissemination Log Standards:

- All secondary dissemination must be tracked for 3 years or until your agency has received an audit.
- The log must contain:
  - The name of the subject of record
  - The name of the person/agency requesting the CHRI
  - The purpose for the request
  - The name of the person releasing the CHRI
  - Date released, and
  - Signature of person receiving CHRI
    - If mailing, document in log.

Dissemination
Examples of authorized entities

- From an ORI to another ORI
  - For same scope and purpose
  - Approved under same legislative authority
- Administrative Hearing Commission (*state agencies*)
  - State agencies should request a closed hearing if fingerprint-based CHRI is part of the record,
  - Information must not be released/disseminated through public hearings
- Attorney General's Office
- Members of State Boards or Commissions

Dissemination - Unauthorized

- Do not disseminate CHRI across state lines.
- Do not store/retain CHRI on a server that is unprotected and is accessible from out of state or by an unauthorized entity.
- Do not disseminate CHRI to a relative, spouse, or friend of the subject of record, etc.
- Do not disseminate CHRI to an independent or third-party auditor, such as a corporate auditor, national program or grant program auditor, etc.
  - Authorized auditors are employees of the Patrol and FBI.

Dissemination - Alternatives

- Clearance letter - indicates the date a background check was conducted and if applicant has met agency qualifications.
- Public Records Request - sent to the Patrol's Custodian of Records.
- Qualification as an Authorized Recipient - a contractor may contact the Patrol to see if they qualify for access (in VECHS, etc.)
- Outsourcing Standard

State Laws Governing Use

- 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.

Federal Laws Governing Use

- 28 CFR 20.33 ... CHRI used only for purpose requested...a current record should be requested when needed.
- 28 CFR 50.12 ... Records may be used solely for purpose requested...cannot be disseminated outside receiving department, related agencies or other authorized entities.

WHAT IS OUTSOURCING?

Outsourcing Functions

- Noncriminal Justice Administrative Functions means "the routine noncriminal justice administrative functions" relating to the processing of CHRI, to include but not limited to the following:
  - Making fitness determinations/recommendations
  - Obtaining missing dispositions
  - Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General last updated 5/15/14
  - Other authorized activities relating to the general handling, use, and storage of CHRI

The Outsourcing Contract

- The contract is between the Authorized Recipient (state agency) and the Contractor providing specific noncriminal justice administrative functions.
- The intent is to require Contractor to maintain a security program in accordance to federal and state laws, the Federal CJIS Security Policy, the Compact Council and US Attorney General.
- Ensures integrity and security of CHRI, subject to all the same requirements as stated in CJIS Security Policy.

How to initiate an Outsourcing Contract

- Initiate a contract with the Contractor outlining the specific duties relating to access of CHRI.
- Submit a letter of request to the State Compact Officer (at the Patrol) for approval prior to allowing any access to CHRI.
- The contract must reference the most current version of the Outsourcing Standard.
  - For assistance, please contact your regional auditor/trainer.

Summary

- Be informed about your state/federal law that gives your agency access to CHRI.
- Be familiar with the contents in your agency user agreement.
- Ensure you are providing Applicant Privacy Rights information to your applicants.
- If retaining CHRI, whether in electronic or physical form, ensure it is protected.
- If disseminating CHRI, ensure it is disseminated in accordance to state and federal law and log it.
- If destroying CHRI, ensure you are destroying in a proper manner.
- Remember, it is your responsibility to protect CHRI from creation to destruction.

Regional Auditor / Trainers

Region 1- West/Northwest and Southwest
Ms. Linda S. Lueckenhoff
(573) 526-6153 extension 2630
Email: Linda.Lueckenhoff@mshp.dps.mo.gov

Region 2 – Central/North and South
Ms. Valerie Hampton
(573) 526-6153 extension 2655
Email: Valerie.Hampton@mshp.dps.mo.gov

Region 3 – East and Southeast
Ms. Pamela Aberle
(573) 526-6153 extension 2625
Email: Pamela.Aberle@mshp.dps.mo.gov

CJIS Division Contacts
Main Number: (573) 526-6153

JD Reece, CJIS Program Manager
Direct Line (573) 522-2151
Email: Jeffrey.Reece@mshp.dps.mo.gov

Kerry Creach, CJIS Program Manager
Direct Line (573) 522-3821
Email: Kerry.Creach@mshp.dps.mo.gov

Carol Kampeter, CJIS Supervisor
(573) 526-6153 extension 2617
Email: Carol.Kampeter@mshp.dps.mo.gov