

803 CMR 7.00: CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

Section

- 7.01: Purpose and Scope
- 7.02: Definitions
- 7.03: Criminal Justice Agency (CJA) Access to Criminal Justice Information System (CJIS)
- 7.04: Background Check Requirements
- 7.05: Maintenance of Municipal and Regional Systems
- 7.06: Global Public Safety Information Agreement
- 7.07: Roles and Responsibilities
- 7.08: Fingerprinting
- 7.09: Prohibited Access to Criminal Justice Information Services (CJIS)
- 7.10: Dissemination of Criminal Offender Record Information (CORI) to a Criminal Justice Agency (CJA)
- 7.11: Logging Requirements for Information Dissemination
- 7.12: Complaints Alleging Improper Access or Dissemination of Criminal Justice Information Services (CJIS) Information
- 7.13: Penalties for Improper Access or Dissemination
- 7.14: Severability

7.01: Purpose and Scope

- (1) 803 CMR 7.00 is issued in accordance with M.G.L. c. 6, §§ 167A and 172; and 28 CFR 20: *Criminal Justice Information System* as it relates to criminal justice information systems maintained by the FBI.
- (2) 803 CMR 7.00 sets forth the roles, responsibilities, and policies that apply to all agencies and individuals either directly accessing the Criminal Justice Information System (CJIS) or using the data obtained from CJIS.
- (3) 803 CMR 7.00 applies to all criminal justice agencies, as defined by both M.G.L. c. 6, § 167, and 28 CFR 20: *Criminal Justice Information Systems*, and to all individuals accessing, using, collecting, storing, or disseminating criminal justice information, including criminal history record information, obtained from CJIS or any other system or source to which Department of Criminal Justice Information Services (DCJIS) provides access.
- (4) Nothing contained in 803 CMR 7.00 shall be interpreted to limit the authority granted to the Criminal Record Review Board (CRRB) or to the (DCJIS) by the Massachusetts General Laws.

7.02: Definitions

As used in 803 CMR 7.00, the following words and phrases shall have the following meanings:

Agency Head. The chief law enforcement or criminal justice official (*e.g.*, Chief of Police, Colonel, Commissioner, Executive Director, *etc.*) at an agency with access to the CJIS or the information contained therein.

Backup CJIS Representative. An employee of a criminal justice agency designated by the agency head to be the agency's secondary point of contact with the Department of Criminal Justice Information Services (DCJIS).

CJIS Authorized User. An employee within a criminal justice agency that is authorized to use CJIS in performance of the employee's official duties.

Criminal Justice Agency (CJA). Pursuant to M.G.L. c. 6, § 167 criminal justice agencies are defined in Massachusetts as, "those agencies at all levels of government which perform as their principal function, activities relating to:

- (a) crime prevention, including research or the sponsorship of research;
- (b) the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or
- (c) the collection, storage, dissemination or usage of criminal offender record information." DCJIS is also required to adhere to the federal definition of criminal justice agency found in 28 CFR 20: *Criminal Justice Information Systems* when granting access to data existing in systems and sources outside of the Commonwealth. 28 CFR 20: *Criminal Justice Information Systems* defines a criminal justice agency as courts and those governmental agencies or any sub-unit thereof that perform 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, including state and federal Inspector General Offices.

Criminal Justice Information System (CJIS). Local, state, regional, interstate and federal information systems, including databases, computer applications and data networks used by criminal justice and public safety agencies to enhance public safety, improve interagency communications, promote officer safety, and support quality justice and law enforcement decision making.

CJIS Representative. An employee of a criminal justice agency designated by the agency head to be the agency's primary point of contact with DCJIS.

7.02: continued

CJIS Systems Agency (CSA). The agency designated by the FBI to provide management control of FBI CJIS systems within a state. DCJIS is the Massachusetts designee.

CJIS Systems Officer (CSO). The individual designated by the CSA within a state who maintains management oversight of FBI CJIS systems on behalf of the FBI. This is an employee of DCJIS.

CJIS Technical Representative. An agency employee designated by the agency head to serve as the technical liaison with DCJIS.

Criminal Record Review Board (CRRB). A statutorily-created board within the Department of Criminal Justice Information Services (DCJIS) that reviews complaints and investigates incidents involving allegations of violations of the laws governing CORI, M.G.L. c. 6, §§ 167A and 172; and 803 CMR 2.00: *Criminal Offender Record Information*.

Department of Criminal Justice Information Services (DCJIS). The Massachusetts public safety agency statutorily responsible for the administration and management of the CJIS.

FBI CJIS Security Policy. The FBI CJIS Division document that describes the security requirements to which all CJIS user agencies must adhere.

Global Public Safety Information Sharing Agreement. An agreement executed between DCJIS and an authorized criminal justice agency that sets forth the rules and responsibilities for accessing and using information maintained within CJIS or shared via the CJIS network.

Initiation of Criminal Proceedings. The point at which a criminal investigation is sufficiently complete that the investigating officer(s) takes action toward bringing a specific suspect to court.

Offense-based Tracking Number (OBTN). A unique identifying number associated with a fingerprint-supported arrest event.

Originating Agency Identifier (ORI). A unique identifier assigned by the FBI CJIS Division to each agency authorized to access or submit data to FBI CJIS information systems.

Person. A natural person, corporation, association, partnership, or other legal entity.

7.02: continued

Public Safety Information System(s). All databases, applications, systems, or network services managed or provided by DCJIS and used by law enforcement and justice officials for authorized criminal justice purposes.

7.03: Criminal Justice Agency (CJA) Access to Criminal Justice Information Systems (CJIS)

- (1) A CJA shall request CJIS access through DCJIS.
- (2) An CJA seeking to gain access to local or Commonwealth criminal justice information systems shall meet the definition of a criminal justice agency as defined in M.G.L. c. 6, §§ 167 and 172(1)(a); and 803 CMR 7.02.
- (3) CJAs seeking access to national criminal justice information systems shall also qualify under the federal definition found at 28 CFR 20: *Criminal Justice Information Systems*. Only those agencies that meet the FBI requirements shall be provided with an ORI.

7.04: Background Check Requirements

- (1) Background checks shall be required for all personnel with access to CJIS. A fingerprint-based criminal history check shall be submitted to the Massachusetts State Police State Identification Section (SIS) and to the FBI for all employees, contractors or vendors with direct terminal or physical access to criminal justice information or criminal justice information systems. This shall include agency personnel or volunteers, state, city or town information technology personnel, and vendors or contractors. These fingerprint-based background checks shall be performed at least once every two years, except for vendor or contractor personnel, who shall be checked annually.
- (2) Individuals with convictions for felony offenses shall not be permitted access to CJIS or any other system or source to which CJIS provides access. If it is found that an individual with access has a conviction for a felony offense, the agency shall notify the CSO at DCJIS. In addition, access privileges shall be immediately terminated. Failure to comply with 803 CMR 7.04 may result in loss of agency access to CJIS or other sanctions by the CSA or FBI.
- (3) Individuals with convictions for misdemeanor offenses may be permitted access to CJIS or any other system or source to which DCJIS provides access, but only upon the approval of the CSO. An agency seeking a waiver shall submit a written request to the CSO at DCJIS.
- (4) Only those users that are authorized by the agency head and have been trained, tested, and certified regarding CJIS policy and compliance may have access to CJIS or to information obtained from CJIS or any other system or source to

which DCJIS provides access.

7.05: Maintenance of Municipal and Regional Systems

Municipal and regional information systems and networks used to access CJIS shall comply with the standards identified within the latest version of the FBI CJIS Security Policy.

7.06: Global Public Safety Information Sharing Agreement

The Global Public Safety Information Agreement shall be executed annually. In addition, an agency shall execute a new Global Public Safety Information Sharing Agreement with DCJIS whenever there are changes to the agency head, the CJIS representative, the backup CJIS representative, or the CJIS technical representative.

7.07: Roles and Responsibilities

- (1) DCJIS shall serve as the FBI CSA for Massachusetts. In this capacity, DCJIS shall be responsible for the administration and management of the FBI CJIS on behalf of the FBI, and shall be responsible for overseeing access to all FBI systems and information by Massachusetts agencies, ensuring system security, training, policy compliance, and auditing.
- (2) The agency head shall be responsible for:
 - (a) designating a CJIS representative, a backup CJIS representative, and a technical representative; the CJIS representative or CJIS backup representative may also serve as the technical representative if necessary;
 - (b) ensuring that all agency users of CJIS, or the information obtained from it, have been trained, tested, and certified within six months of hire and biennially thereafter;
 - (c) responding to audit questionnaires, complaints, and any other inquiries from DCJIS or from the FBI within the time period allowed;
 - (d) providing the results of any investigation into the misuse of the CJIS or any other system or source to which the DCJIS provides access;
 - (e) reporting any misuse of CJIS, including improper access or improper dissemination of information, as soon as possible to DCJIS;
 - (f) executing the Global Public Safety Information Sharing Agreement as required;
 - (g) ensuring that the agency adheres to all CJIS and FBI policies and procedures including the FBI CJIS Security Policy;

7.07: continued

- (h) notifying DCJIS as soon as practicable of any changes in contact information for the agency, the agency head, the CJIS representative, the backup CJIS representative, and the technical representative; and
 - (i) ensuring compliance with all state and federal laws, regulations, and policies related to CJIS and any other system or source to which DCJIS provides access.
- (3) The CJIS representative and the backup CJIS representative shall be responsible for:
- (a) training, testing, and certifying users within six months of hire and biennially thereafter;
 - (b) responding to audit questionnaires, complaints, and/or any other inquiries from the DCJIS or from the FBI within the time period allowed, as well as for providing the results of any investigation into the misuse of the CJIS and any other system or source to which DCJIS provides access;
 - (c) reporting any misuse of the CJIS, including improper access or improper dissemination of information, as soon as possible to DCJIS;
 - (d) executing the Global Public Safety Information Sharing Agreement as required;
 - (e) ensuring that the agency adhere to all CJIS and FBI policies and procedures;
 - (f) notifying DCJIS as soon as practicable of any changes in contact information for the agency, the agency head, the CJIS Representative, the backup CJIS Representative, and the technical representative; and
 - (g) ensuring compliance with all state and federal laws, regulations, and policies related to CJIS and any other system or source to which DCJIS provides access.
- (4) The CJIS technical representative shall be responsible for:
- (a) maintaining and coordinating the agency's technical access to public safety information systems;
 - (b) maintaining CJIS system security requirements;
 - (c) reporting any misuse of the CJIS, including improper access or improper dissemination of information, as soon as possible to a supervisor or

commanding officer; and

7.07: continued

(d) complying with all state and federal laws, regulations and policies related to the CJIS.

(5) The CJIS authorized user shall be responsible for:

(a) use of CJIS for authorized and official criminal justice purposes;

(b) successfully completing all required training;

(c) reporting any misuse of CJIS, including improper access or improper dissemination of information, as soon as possible to a supervisor or commanding officer; and

(d) complying with all state and federal laws, regulations, and policies related to CJIS and to the use of computers.

(6) CJIS certification training shall be completed every two years. In addition, authorized users may be required to complete additional training for specific applications and information systems. This requirement shall apply to any individual who either uses the CJIS directly or who uses information obtained from CJIS or any other system or source to which DCJIS provides access.

(7) CJIS shall be accessed only by trained and certified, criminal justice officials for authorized criminal justice and law enforcement purposes.

7.08: Fingerprinting

(1) Fingerprints shall be submitted to the Massachusetts State Police SIS in the following instances:

(a) criminal justice employment background checks;

(b) criminal arrests by law enforcement agencies;

(c) detentions and incarcerations by the Department of Correction and Sheriffs' Departments (Jail and Houses of Correction); and

(d) licensee screening, specific categories are approved by statute.

(2) Agencies shall submit fingerprints to the FBI via the Massachusetts State Police

(a) to conduct checks of public housing applicants in accordance with 42 U.S.C. 1437d; and

(b) to conduct checks of municipal license applicants in accordance with M.G.L. c. 6, § 172B½.

7.08: continued

- (3) CJAs submitting fingerprints shall comply with DCJIS, the Massachusetts State Police, and FBI policies and requirements for the specific type of check.
- (4) Fingerprints must be submitted for the following:
 - (a) all felony arrests pursuant to M.G.L. c. 263, § 1; and
 - (b) all arrests for felony violations of M.G.L. c. 94C pursuant to M.G.L. c. 94C, § 45.
 - (c) Misdemeanor arrests may be submitted to the SIS where possible.
- (5) All fingerprint submissions shall include an agency-assigned OBTN formatted in the manner prescribed by the SIS.

7.09: Prohibited Access to Criminal Justice Information Services (CJIS)

- (1) CJIS shall not be accessed for any non-criminal justice purpose. The only non-criminal justice purpose for which a user may access CJIS is training. When using CJIS for training purposes, users shall use the test records provided by DCJIS. Users shall not run test records or train with their own personal information or with the personal information of another real individual.
- (2) CJIS shall only be accessed for authorized criminal justice purposes, including:
 - (a) criminal investigations, including motor vehicle and driver's checks;
 - (b) criminal justice employment;
 - (c) arrests or custodial purposes; and
 - (d) research conducted by the CJA.

7.10: Dissemination of Criminal Offender Record Information (CORI) to a Criminal Justice Agency (CJA)

- (1) CORI may be provided to another criminal justice agency for official criminal justice purposes.
- (2) A CJA with official responsibility for a pending criminal investigation or prosecution may disseminate CORI that is specifically related to, and contemporaneous with, an investigation or prosecution.
- (3) A CJA may disseminate CORI that is specifically related to, and contemporaneous with, the search for, or apprehension of, any person, or with a disturbance at a penal institution;

7.10: continued

- (4) A CJA may disseminate CORI to principals or headmasters relating to a student aged 17 or older charged with or convicted of a felony offense, provided that information provided to school officials is limited to the felony offense(s) that may subject the student to suspension or expulsion pursuant to the provisions of M.G.L. c.71, § 37H½; for the purpose of publishing information in the department's daily log as required by M.G.L. c. 41, § 98F;
- (5) A CJA may disseminate CORI as otherwise authorized by law in the interest of public safety.
- (6) Pursuant to M.G.L. c. 6, § 175, a CJA may disseminate CORI to the individual to whom it pertains, or to the individual's attorney, with a signed release from the individual. The CORI provided shall be limited to information compiled by the CJA, such as a police report prepared by the CJA. A CJA may not provide an individual with any CORI obtained through CJIS.
- (7) If an individual seeks to access the individual's national criminal history, the individual shall contact the FBI. Likewise, requests for driver history information shall be submitted to the Massachusetts Registry of Motor Vehicles. All other information contained in CJIS shall only be disseminated to other criminal justice agencies for official criminal justice purposes.
- (8) All requests for an individual's CORI shall be directed to DCJIS.

7.11: Logging Requirements for Information Dissemination

- (1) A CJA that provides information to another authorized CJA, or to an individual employed by an authorized CJA other than the inquiring CJA, shall maintain a secondary dissemination log. The log shall contain the following:
 - (a) subject name;
 - (b) subject date of birth;
 - (c) date and time of the dissemination;
 - (d) name of the individual to whom the information was provided;
 - (e) name of the agency for which the requestor works; and
 - (f) specific reason for the dissemination.
- (2) Motor vehicle owner name and address of a motor vehicle owner may be provided to by the CJA to a tow company only if the tow company has a contract

directly with the CJA; the contract cannot be with the city or town.

7.11: continued

- (a) A CJA shall make an entry into a secondary dissemination log each time it releases information to a tow company.
- (b) In addition to the information identified above, the CJA shall record the registration number and registration state or the vehicle identification number of the towed vehicle in the secondary dissemination log.

7.12: Complaints Alleging Improper Access or Dissemination of Criminal Justice Information Services (CJIS) Information

An individual may file a complaint with DCJIS upon the belief that an agency improperly obtained information, or attempted to obtain CJIS information regarding the individual.

- (a) DCJIS shall review the complaint. If it contains a sufficient statement describing the allegation, DCJIS staff shall conduct an audit of the CJIS system to determine if a specific CJA or CJIS authorized user accessed the individual's information through CJIS during the time period in question. If the audit confirms such access then DCJIS staff may contact the agency head to request an internal investigation
- (b) If requested by the DCJIS, the agency head shall conduct an investigation into the alleged misuse according to the rules, regulations, and policies in place at the agency. At the conclusion of the investigation, the agency head shall provide DCJIS with a written summary of the investigation's findings. In addition, if the agency head substantiates the allegation(s), the written summary shall provide details of the specific actions taken to correct the misuse as well as details of the sanctions imposed on the subject(s) of the investigation, if any.
- (c) DCJIS may impose additional penalties as outlined in 803 CMR 7.00.

7.13: Penalties for Improperly Access or Dissemination

(1) A CJIS user may be subject to federal and state civil and criminal penalties for improper access or dissemination of information obtained from or through CJIS pursuant to M.G.L. c. 6, §§ 167A(d), 168 and 178 and 28 CFR 20: *Criminal Justice Information Systems*.

7.14: Severability

If any provision of 803 CMR 7.00 or the application thereof is held to be invalid, such invalidity shall not affect other provisions or the application of any other part of 803 CMR 7.00 not specifically held invalid and, to this end, the provisions of 803 CMR7.00 and various applications thereof are declared to be severable.

REGULATORY AUTHORITY

803 CMR 7.00: M.G.L. c. 6, § 167A, c. 6, § 172, and 28 CFR 20: *Criminal Justice Information Systems*.

NON-TEXT PAGE