# 803 CMR 7.00: CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

Section



## 7.01: Purpose and Scope

(1) 803 CMR 7.00 is issued in accordance with M.G.L. c. 6, §§ 167A and 172, andin accordance with 28 CFR 20as it relates to criminal justiceinformation systems maintained by the FBI.

(2) 803 CMR 7.00 sets forth the roles, responsibilities, and policies that apply to allagencies and individuals either directly accessing the Criminal Justice Information System (CJIS) or using the data obtained from or through it.

(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, andto all individuals accessing, using, collecting, storing, or disseminating criminaljustice information, including criminal history record information, obtainedfrom or through the CJIS or any other system or source to which theDCJIS provides access.

(4) Nothing contained in 803 CMR 7.00 shall be interpreted to limit the authoritygranted to the Criminal Record Review Board (CRRB) or to the DCJIS by theMassachusetts General Laws.

## 7.02: Definitions

All definitions set forth in 803 CMR 2.00, 5.00, 8.00, 9.00, 10.00 and 11.00 are incorporated herein by reference. The following additional words and phrases as used in 803 CMR 7.00 shall have the following meanings:

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

Backup CJIS Representative. An employee of a criminal justice agency designatedby the agency head to be the agency's secondary point of contact with theDCJIS.

Criminal History Record Information (CHRI).Criminal history record information means information collected nationwide by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

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

Criminal Justice Agency (CJA). Pursuant to M.G.L. c. 6, § 167, criminal justiceagencies are defined in Massachusetts as "those agencies at all levels of governmentwhich 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 rehabilitationof criminal offenders; or

(c) the collection, storage, dissemination, or usage of criminal offender recordinformation."

The DCJIS is also required to adhere to the federal definition of a criminal justice agency found in 28 CFR 20when granting access to data existing in systems and sources outsideof the Commonwealth. 28 CFR 20defines a criminal justice agency as courts and those governmental agenciesor any sub-unit thereof that perform the administration of criminal justicepursuant to a statute or executive order, and that allocates a substantial partof its annual budget to the administration of criminal justice, including stateand federal Inspector General Offices.

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

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

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

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

CJIS User Agreement. An agreement executedbetween the DCJIS and an authorized criminal justice agency that sets forth the rulesand responsibilities for accessing and using information maintained within the CJIS orshared via the CJIS network. As referenced in this regulation, “Global Justice/Public Safety Information Sharing Policy” and “DCJIS Policy” shall be synonymous with CJIS User Agreement.

CJIS Technical Representative. An employee of a criminal justice agency designated by the agencyhead to serve as the technical liaison with the DCJIS.

FBI CJIS Security Policy (CSP). The FBI CJIS Division document that describes thesecurity requirements to which all CJIS user agencies must adhere.

Offense-Based Tracking Number (OBTN). A unique identifying number assigned by a law enforcement or criminal justice agency at the time of booking and associatedwith a fingerprint-supported criminal event.

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

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

7.03: CJA Access to the CJIS

(1) A CJA shall request CJIS access through the DCJIS.

(2) A CJA seeking to gain access to local or Commonwealth criminal justiceinformation systems shall meet the definition of a criminal justice agency asdefined 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 alsoqualify under the federal definition found at 28 CFR 20. Only those agencies that meet the FBI requirements shallbe provided with an ORI.

7.04: Background Check Requirements

(1) State, national, and state-of-residency fingerprint-based background checks shall be conducted on all individuals, including vendors and contractors,with unescorted access to secure areas of a law enforcement or criminal justice agency as required by the CSP. These checks are also required for individuals who have direct access to the CJIS system or to local systems and networks which connect to the CJIS network, such as dispatchers and city/town information technology staff, whether or not they have unescorted access to secure areas.

7.05: Maintenance of Municipal and Regional Systems

Municipal and regional information systems and networks used to access the CJIS or connected to the CJIS network shall comply with the standards identified within the latest version of the CSP.

7.06: CJIS User Agreement and Global Justice/Public Safety Information Sharing Policy

The DCJIS Policy shall be executed annually by each agency with direct access to the CJIS or to the information contained within, or obtained through, the CJIS.In addition, an agency shall execute a new DCJIS Policywith the DCJIS whenever there are changes to the agency head, the CJISrepresentative, the backup CJIS representative, or the CJIS technical representative.

7.07: Roles and Responsibilities

(1) The DCJIS is the FBI CSA for Massachusetts. In this capacity, the DCJISshall be responsible for the administration and management of the FBI CJIS onbehalf of the FBI, and shall be responsible for overseeing access to all FBIsystems and information by Massachusetts agencies, as well as for ensuring system security,training, policy compliance, and auditing.

(2) Each agency head shall be responsible for:

(a) designating a CJIS representative, a backup CJIS representative, and atechnical representative; the CJIS representative or backup CJIS representative may also serve as the technical representative if necessary;
(b) ensuring that all agency users of the CJIS, or the information obtained from it,have been trained, tested, and certified within six months of hire andbiennially thereafter;
(c) responding to audit questionnaires, complaints, and any other inquiries from the DCJIS or from the FBI within the time period allowed;
(d) providing the results of any investigation into the misuse of the CJIS or anyother system or source to which the DCJIS provides access;
(e) reporting any misuse of the CJIS, including improper access to, or improperdissemination of, information, as soon as possible to the DCJIS;
(f) executing the DCJIS Policy asrequired;
(g) ensuring that the agency adheres to all CJIS and FBI policies and procedures, including the FBI CJIS Security Policy;
(h) notifying the DCJIS as soon as practicable of any changes in contact informationfor the agency, the agency head, the CJIS representative, the backup CJISrepresentative, and the technical representative; and
(i) ensuring compliance with all state and federal laws, regulations, and policiesrelated to the CJIS and any other system or source to which the DCJIS providesaccess.

(3) The CJIS representative and the backup CJIS representative shall be responsiblefor:
(a) training, testing, and certifying agency users within six months of hire and bienniallythereafter;
(b) responding to audit questionnaires, complaints, and/or any other inquiriesfrom the DCJIS or from the FBI within the time period allowed, as well asfor providing the results of any investigations into the misuse of the CJIS andany other system or source to which the DCJIS provides access;
(c) reporting any misuse of the CJIS, including improper access to, or improperdissemination of, information, as soon as possible to the DCJIS;
(d) executing the DCJIS Policy asrequired;
(e) ensuring that the agency adheres to all CJIS and FBI policies and procedures;
(f) notifying the DCJIS as soon as practicable of any changes in contact informationfor the agency, the agency head, the CJIS Representative, the backup CJISRepresentative, and the technical representative; and
(g) ensuring compliance with all state and federal laws, regulations, and policiesrelated to the CJIS and any other system or source to which the DCJIS providesaccess.

(4) The CJIS technical representative shall be responsible for:
(a) maintaining and coordinating the agency's technical access to public safetyinformation systems;
(b) maintaining CJIS system security requirements;
(c) reporting any misuse of the CJIS, including improper access to, or improperdissemination of, information, as soon as possible to a supervisor orcommanding officer; and

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

(5) A CJIS authorized user shall be responsible for:
   (a) use of the CJIS for authorized and official criminal justice purposes only;
   (b) successfully completing all required training;
   (c) reporting any misuse of the CJIS, including improper access to, or improperdissemination of, information, as soon as possible to a supervisor orcommanding officer; and
   (d) complying with all state and federal laws, regulations, and policies related to the 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 specificapplications and information systems. This requirement shall apply to anyindividual who either uses the CJIS directly or who uses information obtainedfrom the CJIS or from any other system or source to which the DCJIS provides access.

(7) The CJIS shall be accessed only by trained and certified criminal justice officials forauthorized criminal justice and law enforcement purposes.

7.08: Fingerprinting

(1) Fingerprints shall be submitted to the Massachusetts State Police SIS for criminal justice purposes in thefollowing instances:
   (a) criminal justice employment background checks;
   (b) felony arrests by law enforcement agencies pursuant toM.G.L. c. 263, § 1;
   (c) all arrests for felony violations of M.G.L. c. 94C pursuant to M.G.L. c. 94C,§ 45;
   (c) detentions and incarcerations by the Department of Correction and Sheriffs'Departments (Jails and Houses of Correction); and
   (d) licensee screeningforspecificcategoriesas authorized by ordinance, bylaw,state statute, or federal law and which have been approved by the FBI..

(2) Fingerprints may also be submitted to the SIS for misdemeanor arrests.

(3) CJAs submitting fingerprints shall comply with DCJIS, Massachusetts StatePolice, and FBI policies and requirements for the specific type of fingerprint submission.

(4) All fingerprint submissions shall include an agency-assigned OBTN formatted inthe manner prescribed by the SIS.

7.09: Prohibited Access to the CJIS

(1) The CJIS shall not be accessed for any non-criminal justice purpose. The onlynon-criminal justice purpose for which a user may access the CJIS is training.When using the CJIS for training purposes, users shall use the test records providedby the DCJIS. Users shall not run test records or train with their own personalinformation or with the personal information of another real individual.

(2) The 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;
   (d) civilian employment or licensing purposes as authorized by law and approved by the FBI; and

(e) research conducted by the CJA.

7.10: Dissemination of CORI to a CJA

(1) CORI may be provided to another criminal justice agency for official criminaljustice purposes.

(2) A CJA with official responsibility for a pending criminal investigation orprosecution may disseminate CORI that is specifically related to, andcontemporaneous with, an investigation or prosecution.

(3) A CJA may disseminate CORI that is specifically related to, andcontemporaneous with, the search for, or apprehension of, any person, or with adisturbance at a penal institution.

(4) A CJA may disseminate to principals or headmasters CORI relating to a studentaged 18 or older charged with, or convicted of, a felony offense, provided that the information provided to school officials is limited to the felony offense(s) thatmay subject the student to suspension or expulsion pursuant to the provisions ofM.G.L. c.71, § 37H½.

(5) A CJA may disclose CORI for the purpose of publishing information in thedepartment's daily log as required by M.G.L. c. 41, § 98F.

(6) A CJA may disseminate CORI as otherwise authorized by law in the interest ofpublic safety.

(7) Pursuant to M.G.L. c. 6, § 175, a CJA may disseminate CORI to the individualto whom it pertains, or to the individual's attorney with a signed release from theindividual. The CORI provided shall be limited to information compiled bythe CJA, such as a police report prepared by the CJA. A CJA may not providean individual with any CORI obtained through the CJIS.

(8) If an individual seeks to access the individual's national criminal history, theindividual shall contact the FBI. Likewise, requests for driver historyinformation shall be submitted to the Massachusetts Registry of Motor Vehicles.All other information contained in the CJIS shall only be disseminated to othercriminal justice agencies for official criminal justice purposes.

(9) Any requests for an individual's statewide CORI shall be directed to the DCJIS.

7.11: Logging Requirements for Information Dissemination

(1) A CJA that provides information obtained from or through the CJIS, including CORI and criminal history record information, to another authorized CJA (or to an individualemployed by an authorized CJA) other than the inquiring CJA, shall maintain asecondary 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) The name and address of a motor vehicle owner may beprovided to a tow company only if the tow company has a contractdirectly with the CJA; the contract cannot be with the city or town.

(a) A CJA shall make an entry into a secondary dissemination log each time itreleases information to a tow company.

(b) In addition to the information identified above, the CJA shall record theregistration number and the registration state, or the vehicle identificationnumber, of the towed vehicle in the secondary dissemination log.

7.12 Access to Criminal History Record Informationby Non-Criminal Justice Agencies

(1) The DCJIS may grant non-criminal justice agencies access to Criminal History Record Information (CHRI) in accordance with state and federal laws and regulations.

(2) In order to access CHRI in accordance with applicable law, the non-criminal justice agency head shall be responsible for the following:

(a) executing aNon-Criminal Justice Agency User Agreement with the DCJIS;

(b) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;

(c) executing and providingthe DCJIS with an employee designation form for each employee with direct access to the DCJIS system used to obtainCHRI;

(d) ensuring that all employees with direct access to the DCJIS system used to obtain CHRI have been fingerprinted and have had a complete background investigation in accordance with the latest version of the CSP;

(e) designating a local agency security officer (LASO);

(f) ensuring that all employees with access to CHRI have completed an Individual Agreement of Non-Disclosure (AOND) form;

(f) ensuring that all employees with access to CHRI have completed training;

(f) responding to audit questionnaires, complaints, and any other inquiries from the DCJIS or from the FBI within the time period allowed;

(g) reporting any misuse of CHRI, including improper access to, or improper dissemination of,CHRI, as soon as possible to the DCJIS;

(h) providing the results of any investigation into the misuse of CHRI or any system or source to which the DCJIS provides access;

(i) ensuring that the agency adheres to all DCJIS and FBI policies and procedures,including the CSP;

(j) notifying the DCJIS as soon as practicable of any changes in contact informationfor the agency, including the agency head, local agency security officer,andany employees authorized to access DCJIS systems;

(k) ensuring compliance with all state and federal laws, regulations, and policiesrelated to CHRI, the CJIS, and any other system or source to which the DCJIS providesaccess.

(3) The local agency security officer shall be responsible for the following:

(a) completing the fingerprint-based criminal history background investigation, training, and AOND form;

(b) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;

(c) ensuring compliance with security procedures related to CHRI and DCJIS systems;

(d) coordinating and reporting all personnel security clearance requests and any subsequent criminal history activity relating to an approved employee to the DCJIS CJIS Systems Officer (DCJIS CSO) within five (5) business day.

(e) notifying the DCJIS Information Security Officer (ISO) of any and all security incidents within 48 hours of the discovery of the incident.

(f) responding to audit questionnaires, complaints, and any other inquiries fromthe DCJIS or from the FBI within the time period allowed;
(g) reporting any misuse of CHRI, including improper access to, or improper dissemination of, CHRI, as soon as possible to the DCJIS;
(h) providing the results of any investigations into the misuse of CHRI or any system or source to which the DCJIS provides access;
(i) ensuring that the agency adheres to all DCJIS and FBI policies and procedures, including the CSP;
(j) notifying the DCJIS as soon as practicable of any changes in contact informationfor the agency, including the agency head, local agency security officer, and any employees authorized to access DCJIS systems;
(k) keepingusercodes and passwords used to access CHRI confidential; and
(l) ensuring compliance with all state and federal laws, regulations, and policiesrelated to CHRI, the CJIS, and any other system or source to which the DCJIS provides access.

(4) Employees designated by their agency head to access CHRI shall be responsible for the following:
(a) completing the fingerprint-based criminal backgroundinvestigation (employees with direct access to DCJIS systems and CHRI only);
(b) completing the Individual AOND and training requirements;
(c) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
(d) reporting any subsequent criminal activity to the local agency security officer within 5 days;
(e) keepingusercodes and passwords used to access CHRI confidential;
(f) notifyingthe DCJIS as soon as practicable of any changes in contact information; and
(g) ensuring compliance with all state and federal laws, regulations, and policiesrelated to CHRI, the CJIS, and any other system or source to which the DCJIS provides access.

(5) CHRI shall not be disseminated except in accordance with thelaw that provides the non-criminal justice agency with access to CHRI. In the event CHRI is disseminated, the non-criminal justice agency shall maintain a secondary dissemination log. The log will record the following information:
(a) the subject's name,
(b) the subject's date of birth,
(c) the date and time of dissemination,
(d) the name of the person to whom the CHRI was disseminated along with the name of the organization for which the person works, and
(e) the specific reason for dissemination.

(6) Each entry in the secondary dissemination log will be maintained for a minimum of one year.

(7) Non-criminal justice agencies that are inclined to deny an individual on the basis of his or her CHRI must first provide the individual with information on how to change, correct or update his/her criminal records in accordance with 28 CFR 16.34.

(8) Paper copies of CHRI shall be stored in locked file cabinets and shall not be left unattended.

(9) Electronic copies of CHRI shall be stored in accordance with the provisions of the latest version of the CSP.

(10) CHRI shall only be disposed of in a secure manner. Physical media must be cross-shredded and/or burned, and electronic records mustbe deleted and repeatedly over-written with random 0s and 1s, or the media must be degaussed.

7.13: Complaints Alleging Improper Access to, or Dissemination of,CJISInformation

An individual may file a complaint with the DCJIS upon the belief that an agencyimproperly obtained, or attempted to obtain,CJIS informationregardingthe individual.

(a) The DCJIS shall review the complaint. If it contains a sufficient statementdescribing the allegation, DCJIS staff shall conduct an audit of the CJISsystem to determine if a specific CJA or authorized CJISuser accessed theindividual's information through the CJIS during the time period specified in the complaint. Ifthe audit confirms such access,then DCJIS staff may contact the agency headto request an internal investigation.

(b) If requested by the DCJIS, the agency head shall conduct an investigationinto the alleged misuse according to the rules, regulations, and policies inplace at the agency. At the conclusion of the investigation, the agency headshall provide the DCJIS with a written summary of the investigation's findings.In addition, if the agency head substantiates the allegation(s), the writtensummary shall provide details of the specific actions taken to correct themisuse as well as details of the sanctions imposed on the subject(s) of theinvestigation, if any.

(c) The DCJIS may impose additional penalties as outlined in CJIS policy and these regulations.

7.14: Penalties for Improper Access to, or Dissemination of, CJIS information

(1) An individual found in violation of these regulations, or of DCJIS or FBI policies and procedures, may be subject to federal and state civil and criminal penalties forimproper access to, or dissemination of,information obtained from or through the CJISpursuant to M.G.L. c. 6, §§ 167A(d), 168 and 178, and 28 CFR 20.

(2) Such civil sanctions and penalties may include, but not be limited to, fines issued by the Commissioner of the DCJIS pursuant to M.G.L. c. 6, § 167A(d),

7.15: Severability

If any provision of 803 CMR 7.00, or the application thereof, is held to be invalid, such invalidity shall not affect the 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 CMR 7.00 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: *CriminalJustice Information Systems*.