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, and in accordance with 28 CFR, Part 20 as it relates to criminal justice information systems maintained by the Federal Bureau of Investigation ("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 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, Part 20, and to all individuals accessing, using, collecting, storing, or disseminating criminal justice information, including criminal history record information, obtained from or through CJIS or any other system or source to which the Department of Criminal Justice Information Systems ("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 DCJIS by the Massachusetts General Laws.

7.02: Definitions

All definitions set forth in 803 CMR 2.00: *Criminal Offender Record Information (CORI)*, 5.00: *Criminal Offender Record Information (CORI) - Housing*, 8.00: *Obtaining Criminal Offender Record Information (CORI) for Research Purposes*, 9.00: *Victim Notification Registry (VNR)*, 10.00: *Gun Transaction Recording* and 11.00: *Consumer Reporting Agency (CRA)* are incorporated in 803 CMR 7.02 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 of Police, Colonel, Commissioner, Executive Director, etc.) at an agency with access to CJIS or the information contained therein.

Authorized Criminal Justice Purpose. Any purpose described in the definition of criminal justice agency at M.G.L. c. 6, § 167(a), (b), or (c) which the agency in question is authorized by law to perform and which the user in question is authorized by the agency to perform in the user's official capacity. Authorized criminal justice purposes shall also include use of the Criminal Justice Information System for criminal justice employment and background checks as well as licensing where the criminal justice agency is the licensing authority.

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 DCJIS.

Criminal History Record Information ("CHRI"). Criminal history record information means information collected on individuals by criminal justice agencies anywhere in the United States or its territories, which information consists 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. CHRI 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 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 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.

Pursuant to 28 CFR § 20.3(g), criminal justice agencies also includes courts and any 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, including state and federal Inspector General Offices.

Criminal Justice Information System ("CJIS"). Local, state, regional, interstate, and/or federal information systems, including databases, computer applications, and data networks, used by any criminal justice agency for collecting, storing, sharing, or providing any law enforcement intelligence or any identification or locating information of any individual for criminal justice purposes. This definition specifically includes but is not limited to public safety information systems such as CJISWeb, NCIC, and any law enforcement intelligence database.

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.

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

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. The CSO for Massachusetts is an employee of DCJIS.

CJIS User 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 a CJIS network. As referenced in 803 CMR 7.00, the term "CJIS User Agreement" is synonymous with a "DCJIS Policy."

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

FBI CJIS Security Policy ("CSP"). The FBI CJIS Division document that describes the security requirements to which all CJIS user agencies shall adhere. A copy of this document is publicly available on the FBI CJIS Division's website.

Global Justice and Public Safety User Agreement. An agreement executed between DCJIS and an authorized criminal justice agency that sets forth the rules and responsibilities for accessing and using criminal justice information maintained in systems other than those maintained or shared by DCJIS.

Offense-based Tracking Number ("OBTN"). A unique identifying number assigned by a police department or other criminal justice agency to each arrest event associated with a Massachusetts criminal offense or offenses. The construct of each OBTN shall conform to the format established by the Executive Office of Public Safety and Security. An offender may have multiple OBTN numbers.

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.

Public Safety Information System. Any database, application, system, or network service facilitated, managed, or provided by or through DCJIS and used by criminal justice agencies for any authorized criminal justice purpose.

7.03: CJA Access to CJIS

(1) To access CJIS, a CJA shall request access through DCJIS.

(2) A CJA accessing or seeking to gain access to local or Commonwealth criminal justice information systems shall meet the definition of a criminal justice agency found at M.G.L. c. 6, § 167 and 803 CMR 7.02.

(3) A CJA accessing or seeking to gain access to national criminal justice information systems shall meet the definition of a criminal justice agency found at M.G.L. c. 6, § 167 and 803 CMR 7.02 and shall additionally meet the federal definition of a criminal justice agency found at 28 CFR § 20.3(g) and 803 CMR 7.02.

(4) Only those agencies which meet the definition of a criminal justice agency found at 28 CFR § 20.3(g) and meet any additional requirements imposed by the FBI shall be 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 CJA 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 a CJIS network. These checks are also required for dispatchers and all information technology staff or vendors which work with or service the CJA, regardless of whether such persons are directly employed by the CJA and regardless of whether they have unescorted access to secure areas.

7.05: Maintenance of Municipal and Regional Systems

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

7.06: CJIS User Agreements and Global JusticePublic Safety User Agreements

(1) A CJIS User Agreement shall be executed annually with DCJIS by each agency with direct access to CJIS or to the information contained within or obtained through CJIS.

(2) Each such agency shall execute a new CJIS User Agreement with DCJIS whenever there are changes to the agency head, the CJIS representative, the backup CJIS representative, or the CJIS technical representative.

(3) A CJIS User Agreement may be amended directly or by a memorandum of understanding executed by DCJIS and the relevant agency.

(4) DCJIS may require an amendment or memorandum of understanding to a CJIS User Agreement for any new use or application of CJIS.

(5) DCJIS may require the execution of a Global Justice and Public Safety User Agreement for any agency with direct access to criminal justice information maintained in systems other than CJIS.. Such an agreement may be amended directly or by a memorandum of understanding executed by DCJIS and the relevant agency.

7.07: Roles and Responsibilities

(1) DCJIS is the FBI CSA for Massachusetts. In this capacity, DCJIS shall be responsible for the administration and management of FBI CJIS on behalf of the FBI, and shall be responsible for overseeing access to all FBI systems 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 a technical representative; the CJIS representative or backup CJIS 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 every two years thereafter;
(c) responding to audit questionnaires, complaints, and any other inquiries from DCJIS or from the FBI within the time period specified by DCJIS or the FBI;
(d) providing to DCJIS or the FBI the results of any investigation into the misuse of CJIS or any other system or source to which DCJIS provides access;
(e) reporting to DCJIS as soon as possible any misuse of CJIS, including improper access to or improper dissemination of information contained within or obtained through CJIS;
(f) executing the CJIS User Agreement as required;
(g) ensuring that the agency adheres to all CJIS and FBI policies and procedures, including the FBI CJIS Security Policy;
(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, or the technical representative; and
(i) ensuring compliance with all state and federal laws, regulations, and policies related to CJIS and/or to 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 agency users within six months of hire and biennially thereafter;
(b) responding to audit questionnaires, complaints, and/or any other inquiries from DCJIS or from the FBI within the time period specified by DCJIS or the FBI;
(c) providing to DCJIS or the FBI the results of any investigation into the misuse of CJIS or any other system or source to which DCJIS provides access;
(d) reporting to DCJIS as soon as possible any misuse of CJIS, including improper access to or improper dissemination of information contained within or obtained through CJIS;
(e) executing the CJIS User Agreement as required;
(f) ensuring that the agency adheres to all CJIS and FBI policies and procedures, including the FBI CJIS Security Policy;
(g) 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, or the technical representative; and
(h) ensuring compliance with all state and federal laws, regulations, and policies related to CJIS and/or to 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, including CJIS;
(b) maintaining CJIS system security requirements, including those described in the FBI CJIS Security Policy and any applicable CJIS User Agreement;
(c) reporting to the agency head, CJIS representative, or backup CJIS representative as soon as possible any misuse of CJIS, including improper access to or improper dissemination of information contained within or obtained through CJIS; and
(d) complying with all state and federal laws, regulations, and policies related to CJIS and/or to any other system or source to which DCJIS provides access.

(5) Every CJIS user shall be responsible for:

(a) using CJIS only for authorized criminal justice purposes;
(b) successfully completing all required training;
(c) reporting to the agency head, CJIS representative, or backup CJIS representative as

soon as possible any misuse of CJIS, including improper access to or improper dissemination of information contained within or obtained through CJIS;

(d) complying with all state and federal laws, regulations, and policies related to CJIS and/or to any other system or source to which DCJIS provides; and

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

(6) Every CJIS user and every person who uses information obtained from CJIS or any other system or source to which DCJIS provides access shall:

(a) complete certification training every two years; and

(b) complete additional training as required by DCJIS for specific applications or information systems, or for understanding information therefrom.

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

7.08: Fingerprinting

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

(a) any employment background check for a position with a criminal justice agency;

(b) any felony arrest by a law enforcement agency, as required by M.G.L. c. 263, § 1A;

(c) any arrest for a felony violation of M.G.L. c. 94C, as required by M.G.L. c. 94C, § 45;

(d) detentions and/or incarcerations by the Department of Correction and/or Sheriffs' Departments, including any such detentions and/or incarcerations in jails, houses of correction, or state prisons; and

(e) any screening of a licensee or license applicant for specific categories as 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 State Police, and FBI policies and requirements for the specific type of fingerprint submission.

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

(5) DCJIS may audit any CJA's fingerprinting practices and procedures to ensure compliance with M.G.L. c. 263, § 1A and with these regulations. In connection with any such audit, a CJA is required to respond to audit questionnaires, complaints, and/or any other inquiries from DCJIS within the time period specified by DCJIS.

(6) Fingerprints shall be treated as CJIS information for purposes of 803 CMR 7.00.

7.09: Prohibited Access to CJIS and Prohibited Dissemination of Information from CJIS

(1) CJIS shall not be accessed or used for any purpose other than an authorized criminal justice purpose. CJIS information shall not be disseminated for any purpose other than an authorized criminal justice purpose.

(a) CJIS may be accessed, used, or disseminated for training purposes to facilitate its proper use for authorized criminal justice purposes. When accessing, using, or disseminating CJIS for training purposes, users shall use test records provided by DCJIS. Users shall not access, use, or disseminate other records, nor shall they train with their own personal information or the personal information of any other real individual.

(2) CJIS shall only be accessed or used and CJIS information shall only be disseminated for authorized criminal justice purposes as defined in 803 CMR 7.02. Such purposes may include but are not limited to the following where they otherwise meet the definition of authorized criminal justice purposes provided in 803 CMR 7.02:

(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;
(e) determining the status of a court case for purposes of responding to a public records request; and
(f) research conducted by a CJA.

(3) CJIS shall not be accessed, used, or disseminated in any way that violates any applicable:

(a) statute;
(b) regulation;
(c) policy of the user's agency; or
(d) CJIS User Agreement.

7.10: Dissemination of CORI by a CJA

(1) CORI may be provided to another criminal justice agency for authorized 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 such investigation or prosecution.

(a) CORI shall only be disseminated under this provision upon request by a member of the public when the requestor has identified the individual for whom the requestor is seeking CORI by name.
(b) For the purposes of 803 CMR 7.10(2), the term "contemporaneous" shall mean the following:

1. Time period during which the criminal case is open in court and the information requested is otherwise publicly available in the court file;
2. When the case has been closed, CORI shall only be disseminated under this provision for one year following conviction for misdemeanor offenses and two years for felony offenses.
3. CORI relating to non-convictions and matters not publicly available in the court file shall not be available for dissemination under this provision.

(3) A CJA may disseminate CORI that is specifically related to and contemporaneous with:

(a) the search for or apprehension of any person; or
(b) a disturbance at a penal institution.

(4) A CJA may disseminate to principals or headmasters CORI relating to a student 18 years of age or older charged with or convicted of a felony offense, provided that the information given 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.

(5) A CJA may disclose CORI for the purpose of publishing information in the department'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 of public safety.

(7) 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. When providing CORI in accordance with this paragraph, a CJA may not provide any CORI obtained through CJIS.

(8) 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 authorized criminal justice

purposes.

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

7.11: Logging Requirements for Information Dissemination

(1) A CJA that provides information obtained from or through CJIS, including CORI and criminal history record 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) The name and address of a motor vehicle owner may be provided 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.

(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 803 CMR 7.11(1), the CJA shall record the registration number and the registration state, or the vehicle identification number, of the towed vehicle in the secondary dissemination log.

7.12: Access to Criminal History Record Information by Non-criminal Justice Agencies

(1) 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 a Non-criminal Justice Agency User Agreement with DCJIS;
(b) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
(c) executing and providing DCJIS with an employee designation form for each employee with direct access to the DCJIS system used to obtain CHRI;
(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;
(g) ensuring that all employees with access to CHRI have completed training;
(h) responding to audit questionnaires, complaints, and any other inquiries from DCJIS or from the FBI within the time period specified by DCJIS or the FBI;
(i) reporting to DCJIS as soon as possible any misuse of CHRI or CJIS, including improper access to or improper dissemination CHRI or other information contained within or obtained through CJIS;
(j) providing to DCJIS or the FBI the results of any investigation into the misuse of CHRI or CJIS or any system or source to which DCJIS provides access;
(k) ensuring that the agency adheres to all DCJIS and FBI policies and procedures, including the CSP;
(l) notifying DCJIS as soon as practicable of any changes in contact information for the agency, including the agency head, local agency security officer, and any employees authorized to access DCJIS systems; and
(m) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, CJIS, and/or any other system or source to which DCJIS provides access.

(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 ("CSO") within five business days;
(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 from DCJIS or from the FBI within the time period specified by DCJIS or the FBI ;
(g) reporting to DCJIS as soon as possible any misuse of CHRI or CJIS, including improper access to or improper dissemination CHRI or other information contained within or obtained through CJIS;
(h) providing to DCJIS or the FBI the results of any investigations into the misuse of CHRI or CJIS or any system or source to which DCJIS provides access;
(i) ensuring that the agency adheres to all DCJIS and FBI policies and procedures, including the CSP;
(j) notifying DCJIS as soon as practicable of any changes in contact information for the agency, including the agency head, local agency security officer, and any employees authorized to access DCJIS systems;
(k) keeping user codes and passwords used to access CHRI confidential; and
(l) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, CJIS, and/or any other system or source to which DCJIS provides access.

(4) Employees and other personnel designated by their agency head to access CHRI shall be responsible for the following:

(a) completing the fingerprint-based criminal background investigation (employees with direct access to DCJIS systems and CHRI only);
(b) completing the AOND form and training requirements;
(c) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
(d) reporting any of their own subsequent criminal history to the LASO within five days;
(e) reporting to the LASO as soon as possible any misuse of CHRI or CJIS, including improper access to or improper dissemination CHRI or other information contained within or obtained through CJIS;
(f) keeping user codes and passwords used to access CHRI confidential;
(g) notifying DCJIS as soon as practicable of any changes in contact information; and
(h) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, CJIS, and/or any other system or source to which DCJIS provides access.

(5) CHRI shall not be disseminated except in accordance with the law that provides the non-criminal justice agency with access to CHRI. Whenever CHRI is disseminated, the non-criminal justice agency shall record it in a secondary dissemination log that it shall maintain. The log will record the following information for each dissemination:

(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 make an adverse decision against an individual, which decision is based in any part on the individual's CHRI, shall first provide the individual with information on how to change, correct, or update the individual's 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 shall be cross-shredded and/or burned, and electronic records shall be deleted and repeatedly over-written with random 0s and 1s, or the media shall be degaussed.

7.13: Complaints Alleging Improper Access to or Dissemination of CJIS Information

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

(a) The complaint shall:

(1) be signed by the complaining witness;
(2) state a reasonable time period within which the complaining witness believes the agency improperly obtained or attempted to obtain or disseminated the CJIS information;
(3) state what specific CJIS information the complaining witness believes the agency improperly obtained, attempted to obtain, or disseminated;
(4) state which agency the complaining witness believes improperly obtained or attempted to obtain or disseminated the CJIS information;
(5) state the names and contact information of any persons the complaining witness believes improperly obtained or attempted to obtain or disseminated the CJIS information; and
(6) state any other relevant facts about the allegations.

(b) DCJIS shall review the complaint. If the complaint meets the requirements of 803 CMR 7.13(1)(a), then DCJIS staff shall conduct an audit of the CJIS system to determine if a specific CJA or authorized CJIS user accessed the alleged information through CJIS during the reasonable time period specified in the complaint. If the audit confirms such access, DCJIS staff may contact the agency head to request an internal investigation.

(c) If requested by 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), then 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.

(d) Where there is no violation of the CORI law, DCJIS may close or otherwise dispose of any such complaints by decision of the Commissioner of DCJIS.

(e) Based upon its review of the complaint and any investigation by the agency, and in order to ensure the integrity and security of CJIS, DCJIS may choose to impose preventative measures such as training, restricted access, or other requirements upon the agency or any persons alleged to have improperly obtained, attempted to obtain, or disseminated CJIS information.

(f) DCJIS may impose additional penalties as outlined elsewhere in 803 CMR 7.00, including but not limited to those described in 803 CMR 7.14. Violation of the CORI law may entail additional civil or criminal liability and penalties.

7.14: Penalties for Improper Access to or Dissemination of CJIS Information

(1) An individual found in violation of 803 CMR 7.00, or of DCJIS or FBI policies and procedures, may be subject to federal and state civil and criminal penalties for improper access to or dissemination of information obtained from or through CJIS pursuant to M.G.L. c. 6, §§ 167A(d), 168, 177, 178, and 178½ , as well as 28 CFR, Part 20.

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

7.15: Authority of DCJIS to Maintain Security and Integrity of CJIS

Pursuant to its authority and responsibilities in M.G.L. c. 6, §§ 167A and 172, if DCJIS

detects a possible violation or breach of security associated with a CJIS user or agency, it may immediately deactivate the account of the user or agency pending further investigation and take appropriate action to ensure the security and confidentiality of CJIS information.

7.16: Collection and Submission of Arrest Data for Publication to Website

(1) Pursuant to M.G.L. c. 6, § 167A(i), CJAs shall provide arrest data to Executive Office of Public Safety and Security (EOPSS) and DCJIS in the format consistent with the National Incident-Based Reporting System of the FBI's Uniform Crime Reporting Program ("NIBRS").

(a) All CJAs are subject to this requirement, specifically including but not limited to:

1. the Massachusetts State Police;
2. the Massachusetts Bay Transportation Authority Police Department;
3. any police department in the Commonwealth of Massachusetts or any of its subdivisions;
4. any law enforcement council, as defined in M.G.L. c. 40, § 4J, created by contract between or among cities and towns, pursuant to M.G.L. c. 40, § 4A;
5. any entity employing 1 or more special state police officers appointed pursuant to M.G.L. c. 22C, § 63; and
6. each public or private degree-granting post-secondary institution of higher education as required by M.G.L. c. 6, § 168C.

(b) Each CJA shall submit the required information to EOPSS by electronic means on a monthly basis.

(c) The data fields required for submission shall include all fields required by the FBI NIBRS reporting system and the Massachusetts technical specifications published by EOPSS and DCJIS.

(2) EOPSS will publish de-identified data on a quarterly basis to the internet and submit said information to the FBI.

(3) Criminal justice agencies that fail to submit data in accordance with the law and regulation are subject to sanctions by DCJIS including, but not limited to, mandatory trainings, monitoring, or suspension of CJIS access.

(4) Pursuant to M.G.L. c. 6, § 167A(i)(2), EOPSS and DCJIS shall publish additional guidelines describing:

(a) specific schedules for the submission, transmission and publication of the data;
(b) the specific format for the submission of arrest data;
(c) the categories of arrest data to be submitted, which shall in any event include for each arrest:

1. the name of the arresting authority;
2. the incident number;
3. the alleged offense;
4. the date and time of arrest;
5. the location of arrest; and
6. the race, ethnicity, gender, and age of the arrestee; and

(d) a description of categories of data which constitute personally identifiable information and therefore shall not be posted, not be made available to the public, and not be public records. Such personally identifiable information shall in any event include but not be limited to names and dates of birth of individual arrestees.

7.17: 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, Part 20: *Criminal Justice Information Systems*.