DCJIS Newsletter

James F. Slater, III, Acting Commissioner

IN THIS ISSUE:

DCJIS ANNOUNCEMENTS

Changes to the Massachusetts Missing Persons Law and the CJIS Missing Person (MP) File

On January 7, 2015, Chapter 489 of the Acts of 2014 was enacted. Among other things, this new statute directs the DCJIS to "establish a statewide central register containing all necessary and available identifying information of a missing child". This "central register" must be in place by August 1, 2015. While this is technically not a "new" requirement, the changes to c.22A require that the central register allow for the entry of specific data that is enumerated in the new statute.

The DCJIS will utilize the current CJIS Missing Person (MP) File to satisfy the requirements of the new law. The Missing Person functionality currently existing in the CJIS Messenger client allows for the entry of all the data required by the statute, so no modifications will be necessary. (IMPORTANT: data on location of last contact, the clothing worn by the child, other items that might be with the child, the reason(s) why the reporting party believes the child is missing, the circumstances that indicate the disappearance was involuntary, the circumstances that indicate the child may be at risk of injury or death, and the means of transportation, if any, will need to be entered in the MIS field)

Please see the CJIS Extranet for a detailed summary of the new requirements placed on police departments regarding children who are reported missing as a result of this law, as well as a copy of the statute.

Implementation of FBI Universal Control Numbers (UCNs)

On Tuesday, August 11, 2015 the FBI will be implementing Universal Control Numbers (UCNs) within its Next Generation Identification (NGI) system. The UCN will replace the current FBI Number for the identification of individuals indexed within the NGI.

Historically, the Interstate Identification Index (III) has used FBI numbers to index a subject's criminal record. Under the NGI system, subjects will be indexed based on fingerprint-based identities and will be referenced by an FBI universal control number (FBI UCN).

Critical Points:

- The concept of an FBI Number will cease to exist on 8/11/2015.
- An FBI UCN will be issued to all new NGI records.
- Old FBI Numbers will still exist within NGI, but they will become known as UCNs.
- The concept of an FBI Rap Sheet will cease to exist on 8/11/2015. Instead, "rap sheets" will become known as Identity History Summaries (IdHS).
- The existence of a UCN for an individual DOES NOT MEAN that the individual has a criminal record. Receipt of an FBI UCN under the NGI system simply means the individual has an identity in the NGI system.

Identities in the NGI system will have a unique identifying number, regardless of submission type (e.g., criminal retained fingerprint submissions, civil retained fingerprint submissions, or unsolved latent records). Criminal fingerprint submissions for new identities will be assigned an FBI UCN, and any civil fingerprint submissions that are later submitted and identified as belonging to the same individual will append to this identity/FBI UCN. The NGI system will link criminal and civil records already in existence (legacy identifiers) in the IAFIS and reference the identity using the existing FBI number, which will be referenced as the FBI UCN.

Should you have any questions about this change, please contact the CJIS Support Services Unit via telephone at 617.660.4710 or via email at cjis.support@state.ma.us.

POLICY CORNER

Employer Access to CORI

All employers are authorized under the Massachusetts CORI Law, M.G.L. c. 6, § 172, to access Criminal Offender Record Information (CORI) from the DCJIS iCORI System. It is imperative, therefore, that employers that obtain CORI from the DCJIS or from another source educate themselves regarding the CORI law and regulations (*M.G.L. c. 6, § 168-178B and 803 CMR 2.00 et. seq.).* Many provisions of the CORI law apply to employers that receive CORI from a source other than the DCJIS.

The requirements set forth in the CORI law were promulgated by Chapter 256 of the Acts of 2010 and became effective in May 2012. This article provides a summary of the pertinent provisions of the laws and regulations as they pertain to employers.

Registration and Confidentiality:

Employers that seek to access CORI from the DCJIS iCORI System must register online at www.mass.gov/cjis . The DCJIS has published a reference guide on how to register. The guide is available on the DCJIS website. Organizations that receive a greater degree of CORI access by statute, regulation, or accreditation requirement have their own category to select under the registration options. If your employer type does not appear on this list, please select "Employer" to register as a general employer.

It is important to note that CORI access is subject to many restrictions under state CORI laws. CORI may only be accessed and disseminated as provided by M.G.L. c. 6, § 172. CORI information obtained through the DCJIS iCORI system may only be shared with the subject of the CORI request and staff authorized to access CORI by the employer as outlined in the employer's CORI policy that have a "need to know" this information. Generally, CORI information cannot be shared outside of the employer. Some exceptions apply to this rule. Pursuant to M.G.L. c. 6, § 172 and 803 CMR 2.14, an employer may disseminate CORI in order to defend against an employment discrimination action or to provide CORI to a state agency that licenses or oversees the employer. Dissemination of CORI must be logged in the employer's secondary dissemination log as set forth in M.G.L. c. 6, § 172 and 803 CMR 2.16.

Type of information available from the DCJIS:

The CORI available through the DCJIS iCORI system is provided by the Administrative Office of the Trial Court at the time of court appearance. The CORI database is updated each evening

to reflect the court activity for that day. As such, CORI provided through the DCJIS iCORI system is the record of Massachusetts criminal court appearances and is provided directly from the court system. The CORI response includes a summary of criminal court appearances for the subject. Each offense includes the arraignment date, offense description, offense classification (felony or misdemeanor), disposition type (conviction, non-conviction, or pending), court, and court phone number. Depending on the employer's level of access, the CORI may also include the disposition date and incarceration release date. The CORI records include all Massachusetts criminal court appearances from the age of eighteen and after and those cases where an individual was adjudicated as an adult while under the age of eighteen. Please note: based on a statutory change in the definition of CORI, for arraignments prior to September 2013, the CORI will also include offense where the individual was seventeen years old.

There are three types of CORI access: standard, required, and open. Pursuant to M.G.L. c. 6, § 172, all employers are authorized to receive "standard" CORI access through the DCJIS iCORI system for the purpose of screening employees and volunteers. The DCJIS has interpreted the term "employee" to include the screening of subcontractors or vendors of the employer. As stated, all employers are eligible for this level of access. Prior to the CORI Reform Law amendments, only employers that were either authorized by law or were granted access by the former Criminal History Systems Board (CHSB) could access CORI from the DCJIS.

Some employers are authorized to obtain "required" CORI access. An employer may receive required CORI access if there is a statute, regulation, or accreditation requirement that mandates CORI access. Employers that receive "required" CORI access receive a greater degree of CORI information than those that access "standard" or "open" CORI. Required CORI access is divided into 4 different levels. Required 1 is the lowest level and Required 4 contains the greatest degree of information.

The last category of access is "Open" CORI. Open CORI is the level of CORI information available to the public. Employers are authorized to obtain "standard" or "required" CORI depending on the type of employer. Open CORI may be requested by an employer without the consent of the subject. Therefore, if there is an issue with obtaining a CORI acknowledgment form, the employer may chose to use "open" CORI to access the subject's information. There is less information available under "open" access than under "standard" or "required".

Please visit the DCJIS website at www.mass.gov/cjis for a complete description of the levels of CORI access and a summary of the types of access provided for different types of employers.

CORI Acknowledgment Forms and Verification of Identity:

All employers that request CORI from the DCJIS are required by law to obtain a signed CORI Acknowledgement Form from the subject of the request **prior** to submitting a CORI request for the individual. Furthermore, pursuant to M.G.L. c. 6, § 172 and 803 CMR 2.09, the CORI Acknowledgment Form must be maintained for a period of one year. The CORI Acknowledgement Form contains various fields of information. At minimum, the individual must provide his/her full name, date of birth, and last six digits of his/her social security number in order to process a CORI request. The DCJIS may request a CORI Acknowledgement Form from the employer at any time, including, but not limited to, during the course of conducting an audit or pursuant to a complaint. The DCJIS may also request an acknowledgment form from an employer in order to process the CORI request.

The CORI regulations, 803 CMR 2.09(3), require that, prior to submitting a CORI request, the information on the CORI Acknowledgment Form be verified with a proper form of government-issued identification. Acceptable forms of government identification include a state-issued driver's license, a state-issued identification card, a passport, or a military identification card. If a subject does not possess one of these forms of government-issued identification, please contact the DCJIS legal department to inquire into other acceptable forms of identification. The form of identification used to verify the request must be documented on the CORI Acknowledgement Form. Employers may wish to keep a copy, but are not required to do so under the CORI regulations.

<u>CORI Policy and Opportunity to Dispute Accuracy are not affected by the source of the CORI:</u>

Certain provisions of the CORI law apply to all employers. These requirements are not limited to those employers that solely access CORI from the DCJIS. Pursuant to M.G.L. c. 6, § 171A, employers that conduct five or more CORI checks per year are required to maintain a CORI policy that meets the minimum standards of the DCJIS Model CORI Policy. This requirement applies to all employers and is not limited to those employers that access CORI from the DCJIS iCORI system. Please visit the DCJIS website to obtain a copy of the DCJIS Model CORI Policy.

Furthermore, pursuant to M.G.L. c. 6, § 171A and 803 CMR 2.13, prior to questioning an applicant regarding his or her CORI, an employer must provide the applicant with the CORI. Likewise, pursuant to § 171A and 803 CMR 2.17 and 2.18, if an employer is inclined to make an adverse decision on the basis of a CORI, the employer must also provide a copy of the CORI. This provision applies regardless of whether the CORI was obtained from the DCJIS or another source. The DCJIS has published a model adverse action notification letter than may be used as a template for agencies to notify affected individuals. Please visit the CORI Forms, Applications, and Model Policies section of the DCJIS web site for this information.

Auditing, Complaints, and Sanctions:

The DCJIS reserves the right to audit employers registered to access CORI through the DCJIS iCORI system. An employer may be audited at any time and is responsible for cooperating with said audits. Employers that fail to comply with the audit process may have their registrations revoked in accordance with 803 CMR 2.22.

The DCJIS may also initiate a complaint against an employer that has failed to comply with the CORI laws and regulations. In the case of egregious violations, those cases may be referred for criminal prosecution and are subject to the criminal penalties set forth in M.G.L. c. 6, § 178 (one year in a house of correction or a fine of up to $50,000 for each offense). The DCJIS may also refer complaint investigations for review before the Criminal Record Review Board (CRRB). The CRRB is a Board that has the authority to issue civil sanctions for CORI violations, including, but not limited to, mandated training, compliance reviews, and fines of up to $5,000 for each violation.

Benefits to using the iCORI system:

The CORI law, provides two important exclusions from liability for employers that obtain CORI directly from the DCJIS iCORI system. First, pursuant to M.G.L. c. 6, § 172, employers cannot be found liable for negligent hiring practices by reason of relying solely on CORI received from the DCJIS and not performing additional criminal history background checks, unless required to do so by law; provided, however, that the employer made an employment decision within 90 days of obtaining the CORI and maintained and followed policies and procedures for verification of the subject's identifying information consistent with the requirements set forth in M.G.L. c. 6, § 172 and 803 CMR 2.09.

The second limitation on liability for employers relates to discriminatory employment practices. Pursuant to M.G.L. c. 6, § 172, "…No employer shall be liable for discriminatory employment practices for the failure to hire a person on the basis of criminal offender record information that contains erroneous information requested and received from the department, if the employer would not have been liable if the information had been accurate; provided, however, that the employer made an employment decision within 90 days of obtaining the criminal offender record information and maintained and followed policies and procedures for verification of the individual's information consistent with the requirements set forth in this section and the department's regulations."

Therefore, employers benefit from using the DCJIS iCORI system since they receive the CORI record directly from the court system and the CORI law provides some limitations on liability.

Conclusion:

The DCJIS provides CORI access in accordance with the law as an important tool to ensure public safety. Accordingly, employers must remember that CORI is confidential information that is subject to certain restrictions and procedures under applicable laws and regulations. As such, employers must take the time to ensure that staff that access CORI information have been properly trained and are familiar with the CORI laws and regulations. Violations of the CORI laws and regulations may subject the employer to criminal or civil penalties. The CORI training materials and regulations are available on the DCJIS website at www.mass.gov/cjis. Employers with questions regarding this topic should consult their own legal counsel and may also contact the DCJIS legal department.

DID YOU KNOW?

Validations

Validations are required to be completed monthly. Records which are not validated are subject to removal from the CJIS and NCIC databases.

Please complete your validations by the date indicated by the DCJIS on the notification.

DCJIS Audits

The DCJIS is required, by law and by FBI policy, to audit every agency with access to CJIS or criminal justice information (CJI) on a triennial basis. As part of its audit program, the CJIS Support Services Unit (CSSU) visits each and every site, conducting interviews of agency staff and reviewing internal records.

The DCJIS is currently in the middle of the 2013 audit cycle. If your agency has not yet been audited, and you have questions about the process or required documentation, please call the CJIS Support Services Unit at 617.660.4710.

CJIS Personnel and Security Training Requirements

The FBI CJIS Security Policy and DCJIS regulations require agencies with access to the CJIS to conduct fingerprint-based state-of-residency and national criminal record checks on all personnel with access to CJI once every five (5) years. These checks can be performed via an agency's live-scan fingerprinting device, provided the agency has executed a Civil Fingerprint Submission User Agreement with the Massachusetts State Police State Identification Section (SIS) and the DCJIS.

In addition, agencies are required to train, test, and certify users of CJIS and/or CJI within six (6) months of hire and at least once every two (2) years thereafter. Testing is to be performed using the DCJIS nexTEST online application. Finally, users of CJIS and/or CJI must also undergo CJIS Security Training once every two (2) years. This training is to be conducted via the CJISonline Security Testing Application, which is available at CJISonline.com.

Questions about these requirements should be directed to the CJIS Support Services Unit.

CJIS Best Practice: Using the NIC Number to Verify a Cancel/Clear

A CJIS best practice is to confirm that a CJIS and NCIC record has been successfully cancelled or cleared by conducting an inquiry using the NCIC Number (NIC) of the record.

CJIS Security Policy Requirements for Vendors

The CJIS Security Policy includes several provisions regarding vendors and contractors supplying systems and services to agencies with access to CJIS and FBI systems. Basically, vendors and contractors are required to adhere to the same system and information security provisions of the Policy as law enforcement and criminal justice agencies.

Two of the Policy provisions require special attention by CJIS agencies. First, any vendor or contractor with access to any internal agency system that contains criminal justice information (CJIS) must execute the CJIS Security Addendum, which can be found at the back of the CJIS Security Policy. Each vendor, as well as each individual who is or will be working on an internal agency system, must sign the Addendum. In addition, each vendor employee must also take the CJIS Security Test, which is available at www.cjisonline.com.

Second, any vendor employee with access to systems or networks, or with access to any CJI, or with unescorted access to secure areas of the agency, must undergo a fingerprint-based criminal record check. These checks can be conducted via the agency's live-scan fingerprint device and must be submitted as MAPs.

Any questions regarding CJIS Security Policy requirements for vendors and contractors should be directed to the CJIS Support Services Unit at either cjis.support@state.ma.us or 617.660.4710.

Fingerprint-Based Criminal Record Checks for Municipal Licensing

Municipal police departments that have a by-law or ordinance approved by the FBI may submit fingerprint-based criminal record checks to the State Police State Identification Section (SIS) and to the FBI for individuals applying for municipal licenses. In order to submit these checks, the municipality must first have a by-law or ordinance that has received FBI approval and, if applicable, approval by the Massachusetts Attorney General's Office. The municipality must also have a policy that outlines how the process works, how criminal record information is reviewed and kept, and who has access to this information. For a detailed summary of the requirements and process, and to view and download a model policy, please visit the DCJIS website at www.mass.gov/cjis.

EVENTS & SAVE-THE-DATES

UPCOMING CJIS TRAINING

August 13, 2015

September 17, 2015

October 21, 2015

VALIDATION TRAINING

August 12, 2015

September 23, 2015

October 15, 2015

MIRCS TRAINING

September 10, 2015

Please register for these classes via the CJIS Extranet. Seating is limited, so please register early. You can also register by contacting the CJIS Support Services Unit at 617.660.4710.

WHO TO CONTACT AT DCJIS

Massachusetts DCJIS Contacts

DCJIS Unit	Telephone Number
DCJIS Main Number	617-660-4600
DCJIS Main FAX Number	617-660-4613
TTY Number	617-660-4606
CJIS Support Services Unit	617-660-4710
Firearms Records Bureau	617-660-4782
Firearms PIN & Status Hotline	617-660-4722
Legal Unit	617-660-4760
Constituent Assistance & Research Unit (CARU)	617-660-4640
Criminal Offender Records Information (CORI)	617-660-4704
SAFIS Response Unit (SRU)	617-660-4790
SAFIS Screening Unit	617-660-4721
Victim Services Unit	617-660-4690

MASSACHUSETTS
DEPARTMENT OF CRIMINAL JUSTICE
INFORMATION SERVICES
200 ARLINGTON STREET, SUITE 2200
CHELSEA, MA 02150
MASS.GOV/CJIS

The DCJIS Newsletter will be transmitted electronically and posted to mass.gov/cjis and the DCJIS Extranet.