MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES
GLOBAL JUSTICE AND PUBLIC SAFETY USER AGREEMENT

1.0 Purpose

This Global Justice and Public Safety User Agreement (hereinafter, "Agreement") establishes guidelines for the access, use, dissemination, and sharing of criminal justice information (CJI) collected and maintained within the systems and networks operated, maintained, and managed by the Massachusetts Department of Criminal Justice Information Services (DCJIS).

2.0 Authority

This Agreement is established pursuant to M.G.L. c. 6, s. 167-178B, M.G.L. c. 6, s. 18 ¾, 803 CMR 7.00, and 28 C.F.R. Part 20.

3.0 Scope

This Agreement is applicable to all sworn and non-sworn employees, contractors, interns, volunteers, and information technology support staff of all criminal justice and public safety agencies in the Commonwealth of Massachusetts who utilize or otherwise have access to any software application, system, network, or CJI operated, maintained, or managed by the DCJIS

4.0 Duration of Agreement

This Agreement is in effect until modified or cancelled by the DCJIS. Each Agency Head shall sign off on a copy of this Agreement as a condition of access to the systems and networks operated, maintained, or managed by the DCJIS. In addition, each Agency Head will sign off on a copy of the Companion System Agreement for EACH system for which such an agreement exists. An original, signed copy of this Agreement, along with original, signed copies of any Companion System Agreements, will be kept on file at the DCJIS. The Agency Head shall maintain a copy of the signed agreements. Facsimile and electronic signatures are acceptable as originals.

The Agency Head also agrees to execute a new Global Justice and Public Safety User Agreement and all relevant Companion System Agreements in accordance with 803 CMR 7.06 whenever there are changes to the Agency Head, the CJIS Representative, the backup CJIS Representative, or the CJIS Technical Representative. The new Agreement(s) is/are to be executed within ten (10) business days of the effective date of the change(s) necessitating a new Agreement(s). Original, signed copies of the newly executed Agreement(s) will be forwarded to the DCJIS within ten (10) days of execution.

5.0   Definitions

Authorized User
A sworn or non-sworn justice or public safety employee, contractor, intern, volunteer, or IT support staff member who has been authorized by his/her agency head to access any software application, system, network, or CJI operated, maintained, or managed by the DCJIS

Companion System Agreement
An addendum or "rider" to this Agreement. Each Companion System Agreement establishes rules and protocols for contributing CJI to, or accessing, using, or disseminating CJI from, a specific system or database operated, maintained, or managed by the DCIJS.

Criminal Intelligence System
A system that stores detailed intelligence or investigative information on the suspected criminal activities of subjects and/or which stores only information designed to identify individuals or organizations that are the subject of an inquiry or analysis.

Criminal Justice Information (CJI)
CJI is defined as all data obtained from or through the CJIS necessary for law enforcement and civil agencies to perform their missions. CJI includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information System (CJIS) Representative
The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS-sponsored meetings, seminars, and conferences.

Criminal Justice Information System (CJIS) Backup Representative
The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. The Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

Criminal Justice Information System (CJIS) Technical Representative
The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS

Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

Criminal Justice Information System (CJIS) User-Access Model
A single-identity management model used to authenticate users of the software applications, systems, and networks operated, maintained, or managed by the DCJIS.

Justice and Public Safety Enterprise Application
A software application which criminal justice and public safety agencies use to contribute CJI to, or to access CJI from, databases or systems maintained by or accessed through the DCJIS.

Non-Contributing Agency
An agency that may access CJI from, but which does not contribute CJI to, a database or system operated, maintained, or managed by the DCJIS.

Source Agency
The agency that originally recorded and contributed data to a database or system operated, maintained, or managed by the DCJIS.

6.0 DCJIS Transaction Logs

An audit log of all transactions made by CJIS user agencies is maintained by the DCJIS. This log records the identity of the individual user and agency accessing the system, the date and time of access, and the data entered into, or retrieved from, any database or system operated, maintained, or managed by the DCJIS.

An Agency Head may request a report of all transactions initiated by the users of his/her agency. All report requests must be submitted in writing to the DCJIS.

The DCJIS CSO, at his/her discretion, may, at any time, authorize additional audits of all databases and systems operated, maintained, or managed by the DCJIS.

7.0 Audits of CJI Users

The DCJIS will conduct audits of all agencies, both criminal justice/public safety and non-criminal justice, accessing or using the CJI stored within, or obtained through, the databases, systems, and networks operated, maintained, or managed by the DCJIS. The purpose of these audits is to ensure the integrity and security of the CJI, applications, and systems, to investigate potential inappropriate use of these resources, and to identify potential training needs.

Each CJIS user agencies will be audited at least on a triennial basis (once every 3 years).

8.0 Justice and Public Safety CJI, System, and Network Usage Restrictions

Use of any CJI obtained from or through an application, database, system, or network operated, maintained, or managed by the DCJIS is limited to legitimate justice and public safety purposes within the scope of a user's employment and official duties. DCJIS resources may not be used for personal gain or for personal use, or to assist another individual or entity that is not authorized to access, use, or receive CJI from these resources. Criminal intelligence systems may also be subject to 28 CFR Part 23. Where the provisions of this Agreement or its addenda conflict with 28 CFR Part 23, 28 CFR Part 23 shall supersede this Agreement and its addenda.

9.0 Misuse

An Agency Head is responsible for investigating all alleged incidents or allegations of misuse of any CJI or database, system, or network operated, maintained, or managed by the DCJIS. If an Agency Head determines that someone within his/her agency has misused any of these resources, he/she must, within 10 business days, notify the DCJIS CSO in writing of the circumstances surrounding the misuse, of the actions taken, or to be taken, to address and correct the misuse, and of the policy(ies) and procedures to be implemented to prevent future misuse. The DCJIS CSO may suspend or revoke access to any or all databases or systems operated, maintained, or managed by the DCJIS for the individual(s) involved in the misuse.

Misuse of any DCJIS-provided CJI or resource may result in individual loss of access to the resources, agency loss of access to the resources, and/or state and federal civil and criminal penalties, if applicable. Users are also subject to the rules and regulations of their respective agency.

10.0 Access to DCJIS Resources

Sworn and non-sworn justice and public safety employees, as well as the employees of non-criminal justice agencies, may be granted access to one or more DCJIS applications, systems, and networks as authorized by the Agency head.

Each individual accessing a DCJIS resource will be assigned a unique user identifier (User ID) and initial password. The individual will be required to change his/her password when logging into a resource for the first time. When possible, the same User ID and Password will enable a user to access multiple DCJIS resources. However, some applications may require a separate log in and/or a different User ID and Password.

All passwords used to access a DCJIS resource will meet the DCJIS and FBI security requirements in effect at the time the password is created/changed.

Authorized users shall not share their passwords and user identifications with any other individual. Each authorized user shall be responsible for all transactions conducted with his or her user identification and password.

Agencies are responsible for notifying the DCJIS, in writing, when a user is no longer authorized to access DCJIS resources. DCJIS will terminate or suspend user access depending on the user's status within his/her respective agency.

User IDs and passwords shall be reviewed by each agency on an annual basis. The Agency Head and agency CJIS Representative shall be responsible for this review. The purpose of this review is to confirm the continued authorization of all individuals accessing DCJIS resources. The Agency Head and CJIS Representative shall annually certify the accuracy of his/her agency's authorized user list to the DCJIS CSO.

11.0 Ownership of CJI Contained Within DCJIS Databases and Systems

The Source Agency will maintain ownership of, and responsibility for, the CJI it enters or modifies within any database or system operated, maintained, or managed by the DCJIS.

The Source Agency will exercise due diligence to ensure that the CJI it enters is current, complete, and accurate. Each Source Agency is also responsible for ensuring that the CJI it contributes is in compliance with all federal, state, and local laws.

User agencies shall communicate any errors found in CJI contained in any database or system operated, maintained, or managed by the DCJIS to the Source agency for that CJI as well as to the DCJIS.

12.0 Dissemination of CJI

CJI contained within, or obtained through, any database, system, or network operated, maintained, or managed by the DCJIS shall only be disseminated to other authorized agencies and individuals. In addition, the CJI obtained within, or obtained through, any DCJIS resource shall only be used for authorized justice or public safety purposes.

13.0 Public Records

Records maintained within the databases and systems operated, maintained, or managed by the DCJIS are subject to the Massachusetts Public Records Law as defined in M.G.L. c. 4, s. 7(26).

All responses to public record requests for information contained in a DCJIS resource shall be provided by the Agency that contributed the relevant information.

The DCJIS CSO may respond to a public records request for statistical data drawn from a DCJIS resource.

14.0   Data Submission and Retention Policy

Source Agencies shall contribute data to each DCJIS database or system pursuant to the schedule established in the Companion System Agreement for that database or system, if applicable. Companion System Agreements are attached to this Agreement as Addenda.

Data maintained in DCJIS databases and systems shall be retained pursuant to the schedule established in the Companion System Agreement for that respective system, if applicable.

15.0   Data Submission Standards

For each system that requires the contribution of data by Source Agencies, those Agencies shall submit at least the minimum set of data as established in the Companion System Agreement for the respective subject application.

16.0   Designation of an Agency Representatives

CJIS Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Representative. The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS-sponsored meetings, seminars, and conferences.

Backup CJIS Representative:
Each agency that accesses or uses CJI obtained from or through the systems or networks operated, maintained, or managed by the DCJIS shall also appoint a Backup CJIS Representative. The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. In addition, the Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

CJIS Technical Representative:
Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Technical Representative. The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's

main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

17.0 Technical Support

The Executive Office of Public Safety and Security (EOPSS) Office of Technology and Information Services (OTIS) shall provide technical support services for all applications, databases, systems, and networks, operated, maintained, or managed by the DCJIS.

18.0 Internal Agency Policies

Each agency obtaining CJI either directly from, or through, an application, database, system, or network operated, maintained, or managed by the DCJI shall draft and adopt internal policies to inform and ensure that agency authorized users have read and agree to comply with the provisions of this Agreement and its Addenda.

19.0 Termination of Access

A agency may request termination of its access to one or more DCJIS resources by providing a written request to the DCJIS CSO.

The DCJIS CSO may also terminate access to a DCJIS resoruce pursuant to the terms of a Companion System Agreement.

20.0 Amendments

Any change in the provisions of this Agreement or in the provisions of a Companion System Agreement shall be incorporated by a written amendment approved by the DCJIS CSO.

21.0 Global Justice and Public Safety User Agreement Signoff

By signing this Agreement, the Agency Head acknowledges he/she has read and understood its provisions and that he/she will comply with its terms and conditions.

_____
Agency Head

James F. Slater III
DCJIS Commissioner

_____   9/3/2013
Date   Date