David A. Paterson
Governor

NEW YORK STATE
OFFICE OF CHILDREN & FAMILY SERVICES
52 WASHINGTON STREET
RENSSELAER, NY 12144

Gladys Carrión, Esq.
Commissioner

Local Commissioners Memorandum

Transmittal:	09-OCFS-LCM-10
To:	Local District Commissioners
Issuing Division/Office:	Strategic Planning and Policy Development
Date:	July 6, 2009
Subject:	**Child Protective Services Access to Criminal History Records**
Contact Person(s):	See Contact List on Page 9
Attachments:	Division of Criminal Justice Services: Use & Dissemination Agreement
Attachment Available Online:	No

I. Purpose

The purpose of this Local Commissioners Memorandum (LCM) is to provide local social services districts (local districts) with information about how Child Protective Services (CPS) units can access criminal conviction records of adults who are either named in an open CPS report or residing in the residence of a child named in a report, as permitted by Chapter 602 of the Laws of 2008. This memorandum describes the New York State Division of Criminal Justice Services (DCJS) electronic criminal history record information database that local district CPS units will be able to access, informs local districts about DCJS rules and policies regarding the use of the database and about how local districts can apply to access it, and provides recommendations for the development of protocols to access and use the database.

II. Background

When conducting CPS investigations, local district CPS workers in New York State sometimes have inadequate information on which to base assessments of safety and risk to a child named in a report or other children living in their homes. In addition, although many local district CPS units have developed prudent and sound case practices to address concerns about caseworker safety, CPS units often have had limited means of assessing the potential risk to caseworkers who are making required unannounced home visits to investigate complaints of alleged child abuse or maltreatment.

Chapter 602 of the Laws of 2008 addresses these problems by allowing the manager of a local district CPS unit, or person with law enforcement background who is designated by a commissioner of a local district, to electronically access criminal history record information of persons eighteen years of age or older who are named in a CPS report or who reside in the residence of a child named in a CPS report. Local district CPS staff will be able to consider this information, keeping in mind its limitations, to make timely assessments of potential danger when they receive CPS reports. This will enable local district CPS staff to develop safer responses when conducting investigations. CPS workers will also be able to consider this information in their assessments of child safety and the risk of future abuse or maltreatment.

Chapter 602 adds the category of "child protective services unit" to a list of "qualified agencies," enumerated in subdivision 9 of section 835 of the Executive Law of New York State, that are permitted access to the DCJS criminal history records database in specified circumstances.

Local district CPS units will now have the ability to arrange with DCJS for access to a secure website, eJusticeNY, which contains criminal history record information. Each local district CPS unit doing so will use a code assigned by DCJS, which delineates the type of information it will be able to access under Chapter 602. Local district CPS units will enter identifying information for the individual they wish to search, and will obtain the criminal records of all individuals in the database who meet the criteria of the identifying information. No fee will be charged to local district CPS units to apply for, or to use, eJusticeNY.

III. Program Implications

A. Procedure for Obtaining Access to the Criminal History Records Database

1. Use & Dissemination Agreement

OCFS has provided DCJS with contact information for all local districts, and DCJS will mail each local district commissioner two copies of its Use & Dissemination Agreement (U&D), which is a contract between DCJS and each agency that accesses its criminal history records. The U&D states the duties of DCJS, as well as the duties, responsibilities, and restrictions for the user agency (here, the local district CPS). A local district commissioner who wants a CPS unit(s) in his/her local district to be able to access criminal history records from eJusticeNY must execute the U&D and return it to DCJS.

2. Assignment of Originating Agency Identifier and Access Codes

Upon receipt of a signed U&D from a local district, a DCJS deputy commissioner will also execute the U&D. DCJS will assign that local district an **agency code** and an Originating Agency Identifier (**ORI**). The agency codes and ORIs are unique codes that determine what information will be disclosed to the user requesting electronic criminal history records. DCJS will note the ORI and agency code on Appendix A of the U&D, and a fully executed copy will be returned to the local district. Upon receipt of the U&D, the local district should contact the eJusticeNY Customer Service Group to obtain an eJusticeNY application (contact information on page 9 of this policy).

3. Application to eJusticeNY, and Setup

Application **-** eJusticeNY is an electronic portal program that allows qualified agencies with established U&Ds and ORIs to electronically access the eJusticeNY criminal history record

information database. Any local district that wishes to access this database must complete an eJusticeNY application and submit it to DCJS. If a local district wants to obtain access to eJusticeNY in more than one field office, it must submit a separate application for each of those field offices.

Local districts must provide the following information in their applications for eJusticeNY:

1. Contact information for the user agency, including names and contact information for:
   - the authorizing officer (Commissioner of Social Services, who must also sign the application)
   - the Terminal Agency Coordinator (TAC) – (see "*Set-up*," two paragraphs below)
   - the technical person(s) who will be responsible for IT issues related to eJusticeNY
2. ORI and agency code
3. Type of connection desired (e.g. nyenet, or internet connections, to include a key-like device with a changeable number known as a token, or a branch office solution). Local district staff members should contact the DCJS Customer Service Group Help Desk (800-262-3257, e-mail: cccenter@dcjs.state.ny.us) for explanations and assistance.
4. Names of all persons who will be using the system

Fingerprinting - The local district must conduct a *fingerprint-based* criminal history record search for all persons listed on the eJusticeNY application who will have access to the eJusticeNY database, including the TAC, technicians, and CPS supervisors or other person(s) designated by the local commissioner with law enforcement background. No person may be permitted access to eJusticeNY until the local district has reviewed that person's criminal history search results and approved the individual. Each local district will have to decide, in accordance with the U&D, on its process for reviewing the criminal history record information of persons for whom they would like to allow access to eJusticeNY and for approving such persons. Local districts should contact the DCJS Office of Criminal Justice Operations (Contact Information on p. 9) for questions about fingerprint-based background checks.

Setup – When DCJS has approved a local district's eJusticeNY application(s), DCJS staff will contact the local district to set up approved designated users with access to the eJusticeNY portal on the selected computer terminals. Each local district must appoint a Terminal Agency Coordinator (TAC), who will be responsible for compliance with DCJS regulations and policies in that local district. If a large local district wishes to obtain access to eJusticeNY in more than one CPS field office, then it must designate a TAC for each of those field offices as well as for its central office. All subsequent communications between DCJS and an authorized local district CPS unit will generally be channeled through the TAC.

Training – The TAC must certify that each terminal operator has completed training for eJusticeNY. DCJS provides training on using eJusticeNY and on the confidentiality of information obtained through eJusticeNY. These trainings can be arranged by using the contact information for the eJusticeNY Customer Service Group on page 9 of this LCM. The Customer Service Group can provide training either in live online meetings or through in-person training sessions at DCJS offices in Albany (for up to approximately ten persons). Training takes approximately two hours to complete. Local district staff may also be trained on using eJusticeNY by their TAC.

Cost – There is no fee to apply for eJusticeNY, to access the electronic database of criminal history record information through eJusticeNY, or for the training related to the database. Local districts must pay a fee, currently $75, to fingerprint employees who will have access to eJusticeNY.

B. Description of How eJusticeNY Operates

1. Entering identifying information

An authorized user must enter identifying information about the subject of a search, including name, sex, and date of birth (or estimated date of birth). The user may enter additional information, if known, in several other fields, including race, ethnicity, social security number, height, weight, eye color, and hair color. The more information that is known, the more the search will narrow. **Searches using eJusticeNY are not *fingerprint-based*.**

2. Type of information to be obtained from electronic criminal history searches

The ORI and access codes that will be assigned to local district CPS units will permit them to access criminal history record information that includes convictions and open charges, but not youthful offender adjudications or other sealed records. At the date this LCM is issued, local district CPS units will be able to access only *New York State* criminal records; thus, initially, the criminal history records that CPS units obtain will not include information about *federal* convictions or convictions in *other states*. DCJS is working to obtain access to federal and other-state criminal history record information for CPS units, and expects to arrange for access to national criminal history record information by no later than the end of the year 2009.

The eJusticeNY reports obtained by local district CPS units may contain the following types of criminal record information: identifying information, arrests, detention information, indictments, criminal charges, dispositions (including convictions), and correctional, supervision, and release information. In some cases, the database accessed through eJusticeNY may contain a picture of the individual named in the database. Photographs may or may not be recent.

Note: Chapter 602 only permits access to *conviction records*, but DCJS does not create specialized criminal history records that limit information to convictions. OCFS hereby advises local district CPS units that they may only consider information regarding *convictions* from database searches, and may not consider information regarding *open charges* when making use of information obtained from DCJS. Furthermore, eJusticeNY may sometimes yield information about violations, which are not *criminal* convictions. Information provided by DCJS other than criminal conviction information must be disregarded.

Database searches in eJusticeNY yield criminal history record information for *all* individuals in the database who meet the criteria of the identifying information entered for the search. A search may yield criminal history record information for numerous individuals. If this happens, the user may be unable to distinguish which, if any, of the criminal records apply to the subject of the search.

Because eJusticeNY searches permitted by Chapter 602 are not based upon a *unique* identifier, like fingerprints, there is no way to know with certainty whether a criminal history record found in eJusticeNY applies to a specific individual. (**Note**: It may be helpful to follow up with local law enforcement to determine if an individual is, in fact, the subject of the criminal history record.)

3. Categories of persons that a local district CPS unit is permitted to search

Chapter 602 authorizes local district CPS units to conduct criminal history record searches only for persons who are eighteen or older, associated with an open CPS case, and who are:

- Persons named in a report of suspected or alleged child abuse, maltreatment, or neglect; or

- Persons currently residing in the residence of a child who is alleged to be or suspected of being abused, maltreated, or neglected

DCJS allows persons with access to eJusticeNY to conduct searches for criminal history record information only when they are required to do so in the course of their official duties and responsibilities. The database may not be used to conduct background checks for employees, volunteers, or anyone else, except as may otherwise be permitted by law. It is **never** acceptable for anyone with access to run the name of any person who does not meet the criteria above. Anyone who does so may be subject to prosecution under the New York State Penal Law. If DCJS finds that an agency has abused the use of eJusticeNY, DCJS may terminate its access to the electronic criminal history records database immediately.

4. Required record-keeping of electronic criminal history searches

Each local district CPS unit that uses eJusticeNY is required by DCJS to keep a log of every search that is conducted in the database, which includes identifying information for the person conducting the search, the name of the subject of the search, and the reason for the search. DCJS periodically audits the use of the eJusticeNY system. Audits include a comparison of the names that were searched in eJusticeNY with the names and identifying information in the log.

OCFS strongly advises local districts to devise a protocol for maintaining the logs and for checking that each of the names in the log matches the name of a person associated with a CPS report.

C. Designating Users Who May Access eJusticeNY

Chapter 602 states that access to conviction records is available to a manager of a CPS unit, or to a person with law enforcement background who is specifically designated by the commissioner of the local district for this purpose. DCJS staff has advised OCFS that a local district may extend access rights to several people within these categories. All CPS supervisors are considered, for the purposes of Chapter 602, to be equivalent to a "manager of a CPS unit." With the agreement of a local law enforcement agency, a local district commissioner may designate a person who works for that law enforcement agency to access eJusticeNY for the local district CPS unit.

Every local district will have discretion as to which CPS supervisors or other person(s) with law enforcement background in that local district should be given access to eJusticeNY, and each large local district with more than one field office will also have discretion as to how many of its field offices will have staff authorized to access eJusticeNY. In making these decisions, the local district should consider these factors:

- Number of CPS reports and number of eligible staff
- Number and location of field offices
- Reports received at night and on weekends or holidays
- Maintaining coverage when authorized users are out of the office because of illness, vacation, or any other absence

The local district must list the names of each person who will have access to eJusticeNY in its initial eJusticeNY application(s). The local district is responsible for seeing that each person on the list undergoes a fingerprint-based criminal background check before being permitted access to eJusticeNY. DCJS will assign a person-specific password to each person who is authorized to

access eJusticeNY. The local district is responsible for certifying that each person who will have access to eJusticeNY has been trained on using eJusticeNY and on confidentiality of information.

Whenever a local district subsequently wishes to authorize an additional person to access eJusticeNY, it must complete a fingerprint-based criminal history background check with search and retain status for that person, unless such a check has previously been completed. The TAC must notify DCJS that the local district CPS unit is adding a user in order to obtain a unique password for that person from DCJS. The TAC must also notify DCJS whenever a person who has previously been authorized to conduct eJusticeNY searches will no longer be accessing the system.

While local districts will want to authorize enough persons to access eJusticeNY to be able to conduct as many searches as they think necessary, OCFS recommends that local districts use their discretion to limit the number of persons who will have access.

D. Confidentiality and Restrictions on the Use of Criminal Records Information

1. Confidentiality of criminal history record information

Criminal history record information obtained from eJusticeNY is ***confidential, and may be shared with staff in the local district or with other parties only for child protective purposes.*** The DCJS U&D restricts secondary dissemination of criminal history information received from DCJS, prohibiting the transmission of criminal history record information in any form, printed or otherwise, to another agency or individual, except as necessary for child protective purposes. In signing the U&D, a local district will agree to these restrictions on disclosing or sharing information found in its searches (see the section on Access Restrictions on page 4 of the U&D).

More stringent restrictions apply to the dissemination of the criminal history record information from jurisdictions outside of New York State that local district CPS units are expected to be able to obtain in the future. Federal and other-state criminal history record information is maintained on a national database that can be accessed through eJusticeNY, but which is subject to federal law. Section 151 of the Adam Walsh Law provides that access by governmental social service agencies with child protection responsibilities is to be used only in investigating or responding to reports of child abuse, neglect or exploitation. The federal government authorizes dissemination of this criminal history record information **only** to another **agency** that is an authorized recipient of such information and only for the authorized purpose for which the criminal history record information was originally requested.

Disclosing criminal history record information except as authorized is illegal and such conduct may be prosecuted. If a local district CPS employee breaches the agreement with DCJS regarding confidentiality, DCJS may withdraw the authorization for that agency to access eJusticeNY.

2. Handling of records

DCJS discourages, but does not prohibit, printing out criminal history records. A criminal history record that has been printed out should be destroyed as soon as it is no longer needed for the work of the CPS investigation, unless retention of the information it contains is necessary for child protective purposes.

Similarly, specific criminal history records information obtained from eJusticeNY that local district CPS workers enter into a permanent record, such as CONNECTIONS, should only refer to the

possibility of serious convictions indicated by the eJusticeNY records, which would reflect the limitations of criminal history record information that is not fingerprint-based. CPS workers may, of course, add to the record any other corroborating evidence that they have found.

Search results remain on the eJusticeNY website for a limited period of time.

E. Limitations of Criminal Records Information and Use of the Information

1. Limitations on the reliability of search results

Criminal history record information obtained from eJusticeNY has limitations that should cause local district CPS workers to be cautious when using that information.

One limitation is that the reliability of the criminal history record information obtained depends on the accuracy of the identifying information that is entered. However, the information available to local district CPS units about adults encountered in a CPS investigation is often scant or uncertain. Even identifying information as seemingly certain as a Social Security number is sometimes inaccurate. Also, criminals occasionally provide inaccurate identifying information to law enforcement authorities, which may then be reflected in the eJusticeNY database.

The primary limitation is that, because eJusticeNY searches are not based on the submission of a *unique* identifier such as fingerprints, they do not provide certainty as to whether a criminal history record found applies to a specific individual. An eJusticeNY search permitted by Chapter 602 may yield criminal records for numerous persons who fulfill the search criteria, with no way to determine definitively which, if any, of the criminal history records pertains to the actual person of interest. Even when an eJusticeNY search yields just one criminal record, there may be no means of determining with certainty whether the criminal record actually applies to the person of interest; the criminal record could be that of another individual with the same identifying information, or some of the identifying information entered by the eJusticeNY user may have been inaccurate with regard to the person of interest.

Conversely, the failure to find criminal history record information for the subject of a search may not guarantee that the person in question has no criminal record. If the identifying information is incorrect, the search may not yield existing criminal history record information for the subject. Also, until DCJS arranges sometime later this year for local district CPS units to obtain access to a nationwide criminal history record information database, CPS workers will have no way to know if search subjects have criminal convictions from jurisdictions other than New York State.

Local district CPS units should be aware of the limited reliability of information obtained through name-based searches of the eJusticeNY electronic database.

2. OCFS recommendations on the use of criminal history records information

OCFS believes that information retrieved from eJusticeNY can be helpful in making an immediate assessment of potential dangers to caseworker safety when a CPS worker will be investigating a CPS report. The information may also be helpful in determining safety or risk for a child, and in supporting a determination to indicate a subject, but OCFS recommends caution when using the information for these purposes, particularly in regard to using the information to support a determination to remove a child from the home or to indicate a report. This recommendation is based on the limitations of information obtained from eJusticeNY using a name-based search rather

than a unique identifier such as fingerprints, as noted above, as well as on the need to maintain the confidentiality of the criminal records information.

Caseworker safety

OCFS recommends that CPS workers not rely on eJusticeNY database searches as the only method of assessing the potential of danger in an investigation, but that they continue to employ other careful casework practices that promote safety in conjunction with their searches for criminal records through eJusticeNY.

Local districts may wish to explore developing protocols with local law enforcement agencies that will facilitate obtaining needed assistance quickly when a local district CPS unit obtains information from an eJusticeNY search that causes them to believe that a child may be in a dangerous environment and/or that CPS workers investigating a report may face a potentially dangerous environment.

Assessing safety and risk for children and making CPS determinations

Chapter 602 states, "Child protective services units shall not indicate a report solely based upon the existence of a conviction record." CPS workers should exercise utmost caution when using criminal history information obtained through an eJusticeNY search as a partial basis for indicating a report or for removing a child from a home, because of the limited reliability of the information obtained using a name-based search. CPS workers must always keep in mind that information obtained using a name-based search does not have the certainty of a fingerprint-based criminal history record search and does not constitute proof that an individual has a criminal record. CPS workers will always need to have other evidence that corroborates abuse or maltreatment to indicate a report, and they will always need other evidence demonstrating danger to a child to support other actions to protect a child, such as removal. OCFS recommends that if local district CPS units wish to use criminal history record information from eJusticeNY to assess safety and risk for children, they try to corroborate the information they have obtained from eJusticeNY through other sources, such as law enforcement agencies, courts, family members, and/or other collateral contacts.

CPS workers may disclose criminal history record information that they have obtained from eJusticeNY *only when necessary for child protective purposes*, and should always be mindful of the statutory requirements to maintain the confidentiality of the information.

F. OCFS Role and OCFS-Recommended Protocols

OCFS will have no role in the process of accessing eJusticeNY information by local district CPS units. OCFS is, however, working to add information about the use of eJusticeNY to core training.

OCFS recommends that local districts limit the number of persons who have access to eJusticeNY, consistent with having sufficient staff authorized to enable local district CPS units to conduct searches in a timely manner whenever they are necessary, possibly including during non-business hours.

OCFS recommends that each local district develop a written protocol for procedures to use eJusticeNY, including who makes decisions about when to conduct a search, who will conduct database searches, which computers will be used and where they will be located, and how

information obtained will be handled. Local districts must keep records of all eJusticeNY searches, as required by DCJS.

Local districts accessing eJusticeNY should inform all employees of the confidentiality and privacy considerations surrounding eJusticeNY, including the absolute prohibition of using eJusticeNY for any criminal history record searches other than those authorized by law. OCFS recommends that each local district develop procedures to see that searches are limited to those for persons eighteen years of age or older named in a report of suspected child abuse, maltreatment or neglect, and persons eighteen years of age or older currently residing in the home of a child who is alleged to be abused, maltreated or neglected, which should include matching names on the search log with those of persons named in CPS reports or residing in the home of a child named in a CPS report.

G. Contact Information

DCJS Contact Information

For information about using or applying for eJusticeNY, or obtaining training:

DCJS eJusticeNY Customer Service Group Help Desk
(800) 262-3257, e-mail: cccenter@dcjs.state.ny.us

For information about fingerprint-based criminal history checks:

DCJS Office of Criminal Justice Operations, Mary Stuto
(518) 485-7676, e-mail: Mary.Stuto@dcjs.state.ny.us

OCFS Contact Information

Please contact your Regional Office with any questions:

Buffalo Regional Office	Mary Miller	(716) 847-3145	Mary.Miller@ocfs.state.ny.us
Rochester Regional Office	Linda Kurtz	(585) 238-8201	Linda.Kurtz@ocfs.state.ny.us
Syracuse Regional Office	Jack Klump	(315) 423-1200	Jack.Klump@ocfs.state.ny.us
Albany Regional Office	Kerri Barber	(518) 486-7078	Kerri.Barber@ocfs.state.ny.us
Spring Valley Reg. Office	Patricia Sheehy	(845) 708-2498	Patricia.Sheehy@ocfs.state.ny.us
NYC Regional Office	Patricia Beresford	(212) 383-1788	Patricia.Beresford@ocfs.state.ny.us
Native American Services	Kim Thomas	(716) 847-3123	Kim.Thomas@ocfs.state.ny.us

IV. Effective Date

Chapter 602 of the Laws of 2008 is currently in effect. Local districts wishing to access eJusticeNY may anticipate that the application process will take no more than a few weeks once they submit an executed U&D to DCJS.

/s/ Nancy W. Martinez

Issued By:
Name: Nancy W. Martinez
Title: Director
Division/Office: Strategic Planning and Policy Development

USE & DISSEMINATION AGREEMENT
between
NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES
and
NAME OF AGENCY

Pursuant to Executive Law '837(6) and '837(8-a), the New York State Division of Criminal Justice Services (DCJS) hereby agrees to allow **NAME OF AGENCY, CITY, New York,** the ("User Agency") access to criminal history and wanted and/or missing persons data as may be contained in DCJS and, if applicable, federal Criminal Justice Information Services (CJIS) data files and other state repository files, as available through the Interstate Identification Index (hereinafter referred to as ("III"), in accordance with the following terms and conditions:

DUTIES OF DCJS

DCJS will process authorized criminal history record inquiries, as specified in the Inquiry Specification list (attached hereto and hereinafter referred to as "Appendix A"), by searching its files and returning related criminal history, wanted and/or missing persons information, as permitted by New York State law, DCJS administrative regulations, applicable federal statutes and regulations and CJIS policies and procedures.

DCJS will allow User Agency to access criminal history data electronically by allowing on-line searches of its files and, if applicable, CJIS files for those criminal justice purposes specified in Appendix A, and will return related criminal history, wanted and/or missing person's information, as permitted by New York State law, DCJS administrative regulations, applicable federal statutes and regulations and CJIS policies and procedures.

DCJS will provide such information only to the extent that public funds are made available for that purpose.

DUTIES OF USER AGENCY

User Agency will collect, receive, use and report, when applicable, all information covered by this Agreement in compliance with all applicable state laws and regulations, and all applicable federal laws, regulations, policies and procedures, and restrict inquiries to only those specified in Appendix A. For employment and/or licensing purposes, the User Agency agrees to retain criminal history record information supplied by DCJS only for the duration of the appointment and/or licensing investigation process. Thereafter, such information must be destroyed in a secure manner so as to preclude unauthorized access/use.

For electronic access, the User Agency must have and maintain the necessary computer and associated equipment. In addition to the aforementioned laws, regulations, policies and procedures, the User Agency must also comply with the Electronic Access Guidelines attached as Appendix B. Electronic access allows the User Agency to extract criminal history record information from DCJS criminal history files

and, if applicable, CJIS for inclusion in a separate report, provided such information shall not be compiled by the User Agency into a separate data file for inquiry access or secondary dissemination of any kind.

The User Agency agrees to protect the security of criminal history record information that is contained in either printed or electronic form. All terminals, printers and other electronic devices which allow access to criminal history record information must be in secure locations within the confines of the User Agency. Access to the locations must be restricted to authorized employees, or visitors - such as vendors - necessary for business purposes. Visitors to computer sites or terminal areas must be accompanied by User Agency staff at all times.

The User Agency will familiarize its personnel with, and adhere to, 42 U.S.C. '3789g and the applicable regulations (see, 28 CFR Part 20; Appendix C) and, when applicable, the CJIS Security Policy Issuances, National Crime Information Center (NCIC) Manual and the III Operational and Technical Manual, which are incorporated into this Agreement by reference. The User Agency will also familiarize its personnel with, and ensure adherence to, all physical and personnel security, and other relevant provisions, as specified in the Electronic Access Guidelines in Appendix B. This includes, but is not limited to, provisions concerning the confidentiality of criminal history record information and the physical security of terminals enabled to electronically access the files of DCJS and, if applicable, CJIS.

The User Agency will make records available that support and justify criminal history record inquiries to DCJS and, if applicable, CJIS for the purpose of conducting routine, periodic audits to ensure compliance with all applicable laws, regulations, policies and procedures regarding the information furnished by DCJS, and/or CJIS pursuant to this Agreement. The User Agency agrees to keep such records as DCJS may require including a log of all non-fingerprint inquiries, whether made by electronic and non-electronic means, to facilitate audits. The log will reflect, at a minimum, a record of each inquiry showing the date, time, name of subject, specific reason for the inquiry, file or case number, name of person requesting the inquiry and the terminal operator. In those cases for which an inquiry is made on behalf of another authorized agency, the ORI code of the requesting agency must be recorded. Fingerprint-based inquiries need not be logged.

The User Agency will appoint a Terminal Agency Coordinator (TAC) who will be responsible for ensuring compliance with DCJS and, if applicable, CJIS regulations and policies. The TAC will train and affirm the proficiency of terminal operators who access the criminal history files of DCJS, and, if applicable, the criminal history record files of CJIS, prior to the operator being permitted access. For those User Agencies which access CJIS information, in addition to ensuring that training and testing of each terminal operator has been completed pursuant to NCIC policies and procedures, the TAC will also ensure that DCJS-approved training of each terminal operator has been completed and will maintain each operator's certification attesting to such training for audit purposes. For those User Agencies with access to only NYS criminal history, the TAC will ensure that DCJS-approved training of each terminal operator has been completed and will maintain each operator's certification attesting to such training for audit purposes. The TAC will also maintain a complete, accurate and up-to-date listing of all terminal operators and their user identifications. The head of the User Agency will officially notify DCJS upon the appointment of any TAC by submitting a form supplied by DCJS. The User Agency agrees to provide

sufficient time during normal business hours for the TAC to perform the duties and responsibilities associated with the position, as explained in the *TAC Guidelines (DCJS-EXT 2422).*

The User Agency will conduct fingerprint-based criminal history record/fugitive file searches by submitting fingerprints and the required state, and if applicable, federal fee(s) in accordance with DCJS and CJIS criteria upon initial assignment or employment of all personnel who will have access to DCJS or CJIS criminal history record data, including programmers, technicians and other persons who will be utilized to effectuate access to, or initiate transmission of, DCJS or CJIS data. The User Agency shall not permit access of any kind until the User Agency receives and reviews the fingerprint-based search results and makes a determination if access/employment is appropriate. New York State Correction Law §§752-753 provides factors to be considered in making such determinations. If deemed acceptable, the individual may be granted access. If a felony conviction of any kind is found, access shall be denied and the User Agency will be responsible for immediately notifying DCJS' Office of Criminal Justice Operations (OCJO). Access by an individual with a felony conviction to CJIS information shall be determined pursuant to the federal CJIS Security Policy v. 4.5, December 2008, (Personnel Security 4.5.1.); and access to NYS-only criminal history information shall be determined upon a review and determination by the DCJS Commissioner or his or her designee. The User Agency will be notified upon a completion of such review whether such user shall be permitted access. If an individual approved for access is subsequently arrested, the User Agency will be notified. The User Agency will be responsible for notifying OCJO if such arrest results in a felony conviction. If a felony conviction results from such arrest, the User Agency agrees to review the individual's access in the manner outlined above.

The Information Security Breach and Notification Act (ISBNA) (General Business Law, §889-aa; State Technology Law, §208), requires that state entities, persons or businesses which do business in New York disclose to a New York resident when their private information was, or is reasonably believed to have been, acquired by a person without valid authorization. In accordance with this law, the User Agency shall be responsible for complying with the provisions of the ISBNA and the following terms contained herein with respect to any private information (as defined in ISBNA) received by User Agency under this Agreement that is within the control of the User Agency either on the DCJS information security systems or the User Agency's information security systems (System). In the event of a breach of the security of the System, i.e., the unauthorized acquisition of unencrypted computerized *data* with *private information* (as defined by ISBNA) the User Agency shall immediately notify the Information Security Officer (ISO) of DCJS of any breach of the security of the System immediately following discovery of such breach. The User Agency shall immediately commence an investigation, in cooperation with the ISO of DCJS to determine the scope of the breach and restore the security of the System to prevent any further breaches. Except as otherwise instructed by the ISO of DCJS, User Agency shall, to the fullest extent possible, first consult with and receive authorization from the ISO of DCJS prior to notifying the State Consumer Protection Board, the Office of the Attorney General or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations. DCJS shall be responsible for providing the notice to all such required recipients and for all costs associated with providing such notice. Further, the User Agency will indemnify and hold harmless DCJS for damages assessed against DCJS for breach of security, wrongful disclosure, negligence and any and all causes of action arising out of disclosure of or negligent failure to protect data provided to User Agency from access by unauthorized individuals.

ACCESS RESTRICTIONS

Inquiries for employment and/or licensing purposes via telephone, computer to computer, remote terminal, correspondence or other methods of non-fingerprint inquiry are prohibited. Fingerprints must be submitted for employment and/or licensing purposes.

Secondary dissemination of criminal history record information received from DCJS and/or CJIS is not permitted for any reason unless specifically authorized by law. Secondary dissemination means the transmission of criminal history record information in any form, printed or otherwise, to another agency or individual. In furtherance of their statutory obligations, User Agencies that are the child protective services unit of local social services districts are permitted to access and disclose criminal history record information for child protective purposes.

SUBSEQUENT QUERY REQUIREMENT

If the User Agency has a subsequent need for criminal history record information pertaining to an individual for whom a previous inquiry was made, the User Agency must submit a new inquiry to DCJS to ensure that it has the most up-to-date, complete and accurate criminal history record report available for that individual. A previously obtained criminal history record should never be used again in connection with an extension of the original purpose, or in connection with a new and different purpose. It should be retained only so long as is necessary to document the circumstances of the case/investigation at the time of the inquiry.

Any criminal history record information electronically extracted and saved in a separate report by the User Agency shall not be used in lieu of submitting a new inquiry to DCJS.

SUSPENSION OF SERVICE, CANCELLATION, FINES

DCJS may suspend provision of all/part of the service covered by this Agreement to the User Agency for a known violation of any applicable state or federal law, rule, regulation, policy, procedure, or this Agreement. User Agency recognizes that a known violation of 42 U.S.C. ' 3789g and/or the applicable regulations by the User Agency, or its employees, may subject the User Agency to fines up to $10,000, and may result in suspension of all federal funds. DCJS may resume furnishing any information authorized hereunder when it is satisfied that all violations have been eliminated.

Either DCJS or the User Agency may, on 30 days written notice, terminate this Agreement for any reason.

INDEMNIFICATION OF DCJS

The User Agency, to the extent permitted by State or federal law, agrees to indemnify and save harmless DCJS, its officers and employees, from and against any and all claims, demands, actions, suits and proceedings brought by others arising out of the terms of this Agreement founded upon the negligence or other tortious conduct of the User Agency including but not limited to, any liability for loss or damage by reason of any claim of false imprisonment or false arrest.

VALIDATION OF INACTIVE NON-CRIMINAL FINGERPRINTS

If DCJS retains the User Agency's non-criminal applicant fingerprints in its files for the purpose of issuing reports to the User Agency upon the subsequent arrest of the subject of the retained fingerprints, the User Agency agrees to provide DCJS, at least once every six months, with:

(1) The names and NYSID numbers of individuals whose fingerprints were sent to DCJS for identification processing and retention, but whose applications were not approved for employment or licensure by the User Agency.

(2) The names and NYSID numbers of individuals who subsequently left the User Agency's employment or relinquished licensure.

EFFECTIVE DATE

This Agreement shall supercede any prior Use and Dissemination Agreement between the parties and shall become effective when signed by the Commissioner of DCJS, or his or her designee, and the official of the User Agency having authority to bind the User Agency to the terms and conditions enumerated herein.

NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES	**USER AGENCY: NAME OF AGENCY**
BY_____ Signature	BY_____ Signature
Printed Name: DANIEL M. FORO	Printed Name: _____
Title: DEPUTY COMMISSIONER	Title: _____
Date: _____	Date: _____