

From: Tim Carroll <tc Carroll@greenburghny.com>
Subject: **FOIL request**
Date: August 21, 2012 12:41:22 PM EDT
To: "dberger@nyclu.org" <dberger@nyclu.org>

Hello Daniel Berger,

We have received your FOIL request regarding our License plate readers. We will have a response by August 29, 2012 as to the cost and if any further time will be needed to gather this request.

You have the right to appeal a denial of your application to the Greenburgh Town Board, who shall inform you of their decision in writing within seven days of receipt of such appeal. All appeals to the Town Board should be made through the Office of the Town Attorney, 177 Hillside Ave, White Plains, NY 10607.

Sgt. Tim Carroll
C.O. Records Unit

From: Tim Carroll <tcarroll@greenburghny.com>
Subject: **RE: FOIL Request**
Date: August 31, 2012 6:10:31 PM EDT
To: Daniel Berger <DBerger@nyclu.org>
1 Attachment, 4.4 MB

Hello,

Please see attached file for the records we are providing regarding your FOIL request pertaining to the ALPRs.

Regarding request #3 (e) and (f), we deny the request for locations of ALPR stationary units and the technical capabilities are proprietor to ELSAG.

You have the right to appeal a denial of your application to the Greenburgh Town Board, who shall inform you of their decision in writing within seven days of receipt of such appeal. All appeals to the Town Board should be made through the Office of the Town Attorney, 177 Hillside Ave, White Plains, NY 10607.

Sgt Carroll
Town of Greenburgh Police Department

-----Original Message-----

From: Daniel Berger [mailto:DBerger@nyclu.org]
Sent: Wednesday, August 29, 2012 2:37 PM
To: Tim Carroll
Subject: Re: FOIL Request

Thank you very much.

Daniel E. Berger
Lower Hudson Valley Chapter Director
New York Civil Liberties Union
297 Knollwood Road, Suite 217
White Plains, NY 10607
Tel: (914) 997-7479
Fax: (914) 997-2936

On Aug 29, 2012, at 2:33 PM, Tim Carroll wrote:

Hello,

Pursuant to your FOIL request, I will e-mail documents on Friday August 31, 2012.

Sgt Carroll
Greenburgh Police Department.


[NYCLU FOIL.pdf \(4.4 MB\)](#)

	Town of Greenburgh Police Department		NO.	REFERENCE:
	INTERIM ORDER 188 Tarrytown Road, White Plains, New York 10807		07-04	\$455 Rules & Regulations
			DATE:	November 9, 2007

To: All Department Personnel

Subject: Policy and Procedures relating to the use of the department's Mobile License Plate Reader (LPR).

PURPOSE:

The purpose of this policy is to establish protocols for the usage of the department's Mobile License Plate Reader (LPR) and associated databases.

OVERVIEW OF MOBILE LICENSE PLATE READER:

The mobile LPR is a vehicle mounted system utilizing specialized cameras and computers designed to quickly capture large numbers of photographs of license plates while the patrol vehicle is stationary or moving, during the day or at night and in varying types of weather conditions, convert them to text and compare them to a large list of plates of interest downloaded into the LPR from the New York State Police Information Network (NYSPIN). In addition to facilitating the recovery of reported stolen vehicles and license plates, an LPR can detect a motor vehicle driven by an operator that has a suspended or revoked driver's license, or a motor vehicle insurance violation or a registration that is suspended or revoked. In addition, the unit can be used to detect vehicles involved in Amber Alerts or those that have been targeted in criminal investigations or to discover suspect vehicles. The system operates at speeds fast enough to capture all license plates that they come in contact with so that the number of plates read is limited only by the number of vehicles within range of the cameras.

The LPR equipment affords access to two files provided through the New York State Police Information Network (NYSPIN) to the department, which is downloaded through TraCS on a daily basis. One file contains information on stolen vehicles, stolen plates, wants and warrants connected with the plate and suspended or revoked registrations relating to New York State while a second file, lists national stolen vehicles and plates as well as warrants associated with the plate. Canadian entries through NCIC are also included in this file. Deployment of the LPR equipment is primarily intended to provide access to these files to facilitate enforcement of the Vehicle and Traffic Law and Penal Law, and for the furtherance of criminal investigations. Use of the LPR equipment is restricted to this purpose. No officer may use, or authorize the use, of the LPR equipment or database for any other reason. Except as described under Subdivision III(6) and V of this Procedure, this includes the

proactive entry of any information into the database without the permission of one of the staff officers mentioned in this Procedure. A request for use of the LPR equipment or for access to the database beyond the reasons specifically cited in this Procedure, may be made to the Chief of Police, or in his absence, his designee, or the Patrol Division Commander, who shall administer and oversee the LPR program. Any such request shall be made in writing, unless the use is for an emergency purpose, that might be compromised if written authority was sought. In such a case, verbal approval followed as closely as practical by a written request will be satisfactory.

I. LPR ADMINISTRATION:

The Commanding Officer of the Patrol Division shall administer and oversee the LPR Program. His/her responsibilities shall include:

1. Maintaining an adequate number of individuals qualified to train department personnel in the use of the LPR equipment and databases;

2. Selection and training of all approved members in the operation of the LPR system and ensuring that all training is appropriately documented in department records;

Note

Officers are **prohibited** from using the LPR system until they have been properly trained and certified in its use and have familiarized themselves with the operational protocols outlined in this Procedure.

3. Arranging for additional training when deemed necessary; and

4. Maintenance of records identifying approved LPR details and their results and ensuring that appropriate documentation of significant incidents and arrests related to LPR usage are made;

5. Preparation and forwarding of the Quarterly License Plate Reader Progress Report to the New York State Division of Criminal Justice Services;

6. Arranging for the repair or reinstallation of the LPR when necessary.

II. LPR OPERATOR SELECTION:

The following qualifications shall be considered when selecting/approving members for LPR training:

1. The members driving record;

2. Past demonstration of good judgment in connection with vehicle pursuits;

3. Good working knowledge of the Vehicle and Traffic and Penal Laws and a positive history of enforcement of these laws.

III. PATROL OPERATIONS:

Only officers trained and certified in the use of the LPR system shall be assigned to vehicles equipped with a license plate reader. Normally, these assignments shall be made through the office of the Patrol Division commander. Vehicle(s) equipped with an LPR should be employed as often as practical. Absent mechanical difficulties and/or a lack of trained personnel, at a minimum, this shall be five tours per week. The following guidelines shall apply to use of the LPR.

1. A "Daily License Plate Reader Log" (UF 135) shall be prepared by each officer assigned to a vehicle equipped with an LPR. The log shall contain the name(s) of the officer(s) assigned, the tour and assignment. Data shall also be entered into the log reflecting the number of arrests, recoveries, summonses issued, etc., based on LPR hits. The completed Daily Log shall be forwarded to the office of the Patrol Division Commander along with a copy of the Incident Report associated with any arrest made in connection with an LPR hit. This/these shall be prepared in addition to any other paperwork (i.e., radar log, Activity Sheet, UF10) that the officer is normally required to prepare. Daily License Plate Reader Logs that do not reference and arrest must be maintained for a minimum period of the current year plus one. Logs containing arrest information must be retained a part of the Arrest Case file and maintained until all arrests associated with the log page have reached a final disposition. In the event a log contains multiple arrests, the arresting officer shall ensure that copies of the original are clearly indicated as such by checking the word "Copy" at the bottom of the Log and completing the line indicating in which Arrest Case file the original resides.

2. The LPR provides an audible alarm and displays a picture on the computer screen of a suspect plate that is read and compared to its database. The LPR software will also display the reason for the alarm (i.e., Suspended/Revoked, Stolen, Wanted, etc.) on the screen and the state or Canadian province associated with the "hit".

Note

Prior to stopping a vehicle based on an LPR hit, Officers must verify that the state of the wanted plate matches the state of the vehicle displayed on their screen.

3. **Hit Verification** - The information received from license plates recognized as wanted hits is dated, typically up to 24 hours old. Therefore, all hits received through the LPR System must be verified through NYSPIN as presently outlined in department policies and procedures. Hits received against department entered plates should be verified through the appropriate channels (i.e., Originating Hot Line Agency, Detective Division, etc.).

4. **Unoccupied Vehicles (Verified Hits)** - When verification of a stolen, wanted or suspect vehicle hit is received for a vehicle

that is **unoccupied**, the operator of the LPR equipped vehicle shall, while maintaining visual observation of the vehicle, immediately contact a supervisor to determine what further action shall be taken (i.e., continued surveillance or immediate recovery).

5. **Updating LPR Wanted Files** - At the beginning of each special detail or tour on which the LPR is to be employed, a "start-shift" from the TraCS application shall be conducted to update and transfer the required files to the vehicle's computer.

6. **User Added Hit Files** - Should it become necessary to add specific information to the database once the initial upload has been completed, the officer may do so by manually entering the information. This option should be utilized in cases where crimes are reported subsequent to LPR deployment. Information of this nature that **must** be added shall include:

- a. Amber Alert and NYS DCJS Missing Child/College Student information received through NYSPIN, facsimile, email or other notification system;

Note

Upon notification of an Amber Alert or Missing Child, the LPR operator shall immediately enter the license plate into the LPR database and then promptly search the database to see if a previous record exists. A supervisor shall be contacted immediately if a record of a previous encounter is found to determine what course of action shall then be taken.

- b. Vehicles reported Stolen from within Greenburgh;
- c. Wanted/Missing persons connected with a vehicle;

The LPR operator may also opt to add information on:

- c. Suspect vehicle information received over the county Hot Line;
- d. Radio broadcasts of suspect vehicles wanted in connection with local crimes;

Note

Whenever additional information is added to the database, the appropriate comments describing the reason for the want shall be added under the Remarks section (i.e., "wanted for questioning only in connection with a burglary" or "wanted in connection with an armed robbery, firearm displayed").

Note

Whenever a new license plate is entered into the LPR database, an entry **must** be made on the Daily License Plate Reader Log.

- e. Manual plate checks may also be performed against the database.

7. **Traffic Stops** - Officers assigned to LPR equipped vehicles should be aware that some LPR-based stops will involve misdemeanor and felony criminal offenders. When making such stops, officers will take all necessary precautions to ensure their personal safety and that of the public. Department regulations affecting stops of this nature shall be strictly adhered to. In addition, officers shall be mindful of the following.

- a. All traffic stops based on an LPR alarm will be made in a safe manner in accordance with department regulations.
- b. Officers should recognize that many of the LPR-based vehicle stops will involve vehicles that are on-coming in traffic to the direction of travel of the patrol unit. This will require the execution of a U-turn to perform. Sufficient care must be exercised by the operator in carrying out this maneuver to avoid collisions and minimize the danger to other motorists and pedestrians.
- c. Department **Pursuit** policy strictly applies to vehicles fleeing an attempted traffic stop that was initiated as a result of an LPR alarm. Supervisory personnel shall immediately determine the nature of the alarm when such a pursuit is initiated.

IV. SPECIAL DETAILS:

The LPR can be used for many purposes other than those identified as routine patrol. These can include:

- 1. To further criminal investigations by assigning the LPR equipment in a designated manner or area and by providing access to stored records gathered during these activities.

Note

Requests to view stored data shall be recorded on the LPR Data Query Log, which shall be maintained in the same manner as a Criminal History Log for a period of the current year plus one. Access shall be limited to the Patrol Division Commander, Detective Division Commander, Commander of the Special Investigation Unit or the department's Field Intelligence Officers. The officer making the inquiry must make the log entry. If the log has an arrest hit associated with it, it must be retained as part of the Arrest Case file. Logs should be retained until all arrests associated with the log page have reached a final disposition. See policy under Subdivision II(1) of this Procedure if duplicate copies of the log for multiple

case files is required.

2. Loading specific files in to the LPR that may relate to a situation of concern to a specific geographical area (i.e., the plate numbers of gang members, burglary or robbery or other types of criminal suspects).

3. Saturation patrols in areas where narcotics, auto theft, fraudulent documents and gun and gang offenses are suspected and during which all vehicles generating verified LPR hits are stopped.

Note

Additional staffing and possibly support personnel (i.e., K-9 and Street Crime Officers) as well as a second LPR officer to verify hits through NYSPIN should be considered when engaging in activities that are likely to result in an increased hazard to police personnel.

Approval for these details must always be obtained from the Commanding officer of the Patrol Division or the Chief of Police prior to their execution.

V. MUTUAL AID SITUATIONS:

There may be occasions where the use of this department's LPR can assist another agency in locating an abducted or missing child or in apprehending a criminal suspect by assisting in a coordinated search of a particular area for the suspect plate. When such a request for assistance is received, the Patrol Division Commander or in his absence the Chief of Police shall be contacted to secure approval to assist. Should approval be granted, two LPR certified officers shall be assigned to an LPR equipped vehicle to assist. They shall add the target plate number to the LPR database. One of the assigned officers shall operate the vehicle while the second officer verifies any hits. Of course, there may also be situations in which Greenburgh may request assistance from another agency's LPR for the same purpose.

VI. MAINTENANCE AND SECURITY:

1. The LPR cameras need not be removed during the period a vehicle is out of service for routine maintenance (i.e., oil changes, tire replacement, brakes, radio repair). However, if the vehicle is going to be out of service for more than a week or is being taken off line, the Commanding Officer of the Patrol Division shall ensure the unit is removed and installed on a suitable department vehicle.

2. The LPR cameras need not be removed for the purposes of running an LPR-equipped vehicle through an automatic car wash.

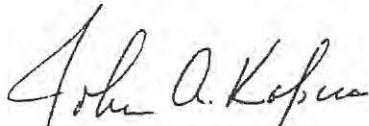
3. Officers may use a damp cloth to clean the surface of the trunk-mounted cameras if they become excessively dirty and performance suffers.

4. Officers shall immediately document any problems with the LPR equipment and/or software on a UF100 and forward the report to the Commanding Officer of the Patrol Division.

5. All unattended vehicles should be locked and turned off.

VII. LEGAL CONSIDERATIONS:

There does not currently appear to be any legal impediment to the use of a License Plate Reader by law enforcement. Legal research seems to convincingly indicate that no fourth amendment considerations exist through a police officer observing a license plate on a car viewable from a public street through the use of an LPR, since an LPR merely accomplishes, in a much more efficient manner, the same task that an officer could accomplish by reading a plate and manually entering it into a database.



John A. Kapica
Chief of Police

	Town of Greenburgh Police Department INTERIM ORDER 188 Tarrytown Road, White Plains, New York 10607	NO. 09-07	REFERENCE: 455.04 Rules & Regs.
		DATE: 10/27/09	

To: All Sworn Personnel and Dispatchers

Subject: Enforcement of Article XII of Chapter 460 of the Greenburgh Code entitled the "Scofflaw Program".

Pending revision of the department's Rules, Regulations and Manual of Procedures, the following policy shall guide department members when enforcing Article XII of Chapter 460 of the Greenburgh Code. This Order shall take effect immediately.

Background:

In May 2009, the Greenburgh Town Board adopted a new Article in Chapter 460 of the Greenburgh Code entitled the "Scofflaw Program". The intent of the new Article was to curtail the number of motorists who failed to respond to parking tickets issued against their vehicles, and in response to a report that \$2.7 million in fines and penalties was owed to the Town by the registered owners of vehicles who had failed to answer parking tickets that had been issued against their vehicles. Subsequent to the adoption of the law, Complus, the firm that administers the Town's parking ticket program, was directed to send out warning letters to all vehicle owners who would be classified as Scofflaws under the program and whose vehicles were ticketed within the past three years. A few of those individuals contacted the Court in response to those letters. The next phase of the program is to begin enforcement of the law by towing and impounding the vehicles of Scofflaws found parked on public streets and parking lots within the Town of Greenburgh.

PURPOSE:

To prescribe a course of action which members of this department shall follow in enforcing the Town's "Scofflaw Program".

I. POLICY:

As described in this procedure, it shall be the policy of the Greenburgh Police Department to aggressively enforce the Town's "Scofflaw Program" as codified under Article XII of Chapter 460 of the Greenburgh Code.

II. DEFINITIONS:

1. **Scofflaw:** The registered owner of a vehicle against which three or more parking summonses have been issued, at least two of which have been issued on separate dates, and a minimum of three of which remain unanswered for a period of forty-five (45) days of the appearance date or dates on such summonses.

III. PROCEDURE:

1. **Background:** The Town of Greenburgh presently employs Complus Data Innovations, Inc. of Tarrytown to manage its parking ticket program. Parking tickets are issued by employees of the Hartsdale Public Parking District using electronic hand-held devices, while department members utilize paper tickets. The data in the electronic hand-held ticket writing devices is uploaded daily to Complus while paper tickets are forwarded to them by mail on a Monday through Friday basis. Complus maintains the database of all parking tickets which Court personnel may access when a person comes in to answer their ticket(s). Court personnel

may enter information on the fine paid or place a "Hold" on the ticket(s) in the event the person pleads "Not Guilty" or enters into an arrangement with the Court to pay the fines and/or penalties. By doing this, penalties will not accrue and if the vehicle is a designated Scofflaw, a "Hold" will be indicated in the ticket history signifying the vehicle should not be towed.

2. **Scofflaw Information:** The Complus database is updated when the information in the electronic handheld ticket writing devices is uploaded and by hand when paper tickets are received. The database is also dynamically updated when Court personnel enter payment of fines or holds. Scofflaw information is downloaded to the handheld devices during the information transfer. The Scofflaw information in the department's License Plate Reader is updated daily Monday through Friday of each week.

3. **Notification of Potential Scofflaw Hit:** The majority of Scofflaw hits will be generated by Parking Enforcement officers when writing a ticket for a car in violation and by the police officer(s) operating the Department's LPR equipped enforcement vehicle. A second LPR is expected to be purchased before the end of 2009.

NOTE

**Because confirmation of a Scofflaw hit is required,
initially Scofflaw enforcement shall only take place Monday
through Friday exclusive of holidays and days when the
Town Court and Complus are closed for business.**

4. **Parking Enforcement Officer:** When a Parking Enforcement officer obtains a Scofflaw hit, (s)he shall notify Police Headquarters that a hit has been obtained and provide the dispatcher with a complete description of the vehicle, including make, model, color, registration number and location that it is parked. The Parking Enforcement officer shall remain at the vehicle's location until the arrival of a police officer.

5. **Dispatch Personnel:** Upon notification by a Parking Enforcement or Police officer that a potential Scofflaw hit has been obtained, Dispatch personnel shall:

a. Enter the call into CAD and dispatch a police officer to the location if necessary.

b. Until Complus database session software is secured and loaded on a computer in the Communications section, place a call to Complus at 914 747-1200 to confirm that the vehicle continues to be listed as a Scofflaw in their database. Complus will confirm the number of unanswered tickets, the dates they were issued and the amount of fines and penalties owed. Once the Complus database session is secured, rather than contact Complus by telephone, Dispatch personnel will query the Complus software to obtain this information.

NOTE

**The Department will be securing a Complus database session
that will be installed on a computer in Communications. Since
this will provide direct access to the same database that Complus
personnel would query, it will no longer be necessary to contact
Complus by telephone to confirm the hit.**

c. Once it has been confirmed that the hit is valid either through a call to Complus or a check of the Complus database, the Town Court shall be contacted to ascertain if any payments were received for the vehicle in question that were not yet entered into the Complus database or if a "Not Guilty" plea was accepted that was not yet entered as a "Hold" in the system.

NOTE

**The intent of steps b. and c. under this section are primarily to make
doubly certain the vehicle in question remains a Scofflaw so as to
minimize the possibility that a vehicle is erroneously towed and
secondarily, as discussed more fully further on in this Procedure,
to provide the Desk Officer with the information required to
determine the amount of security that should be posted by the
vehicle's owner to secure its release.**

- d. Provide the Desk Officer and Police Officer with confirmation of the hit or otherwise.
- e. Utilizing the Rotating Tow List, contact the next tow company on the list to remove the vehicle for which confirmation has been received providing the necessary information to ensure the proper tow vehicle is dispatched.

NOTE

**ALL vehicles towed under the Scofflaw Program shall
be brought to the Police Headquarters Impound Lot**

- f. Enter the vehicle in the NYSPIN computer system as an impound (IENT)
- g. Subsequent to a Police Supervisor accepting security on an impounded Scofflaw vehicle and completing a UF 138 Hold on Scofflaw Status form, fax completed form to the Town Court at 682-5378 and enter the name and computer ID number of the dispatcher faxing the UF 138 in the appropriate field on the form.

6. **Patrol Personnel:** When a Police officer assigned to a vehicle equipped with a License Plate Reader obtains a Scofflaw hit, (s)he shall immediately advise communications and request that they take the necessary steps to confirm the vehicle continues to be a Scofflaw, and:

- a. Issue summonses for any violations that are noted.
- b. Prepare a Police Report fully describing the vehicle (i.e., registered owner, address vehicle make, model and registration number), the circumstances under which it was discovered and indicating the findings of the confirmation process. This should include a statement supporting that the vehicle qualifies as a Scofflaw by indicating the number of outstanding summonses, the total amount of fines and penalties due and specifically mentioning the dates on which three of the summonses were issued ensuring that they are 45 or more days past the date that they should have been answered by and that at least two of them were issued on separate dates (see Section II Definitions). The name of the Tow Company responding should also be entered into the report. For example; "A blue, 2004 Honda Pilot bearing NY registration ABC123 expiring on November 30, 2010 and registered to Joe Smith, 123 Anywhere Street, Hartsdale, N.Y. 10530, discovered illegally parked on the third level of Site A (no money in meter). Check of Complux database indicated 17 unpaid tickets and \$1,500 outstanding in unpaid fines and penalties. Three tickets issued on January 2nd, 3rd, and 4th, 2007. Communications confirmed vehicle remains a Scofflaw. Summons issued for meter parking violation and vehicle removed by RJT Towing to headquarters impound lot."
- c. Standby until arrival of the tow truck and accompany the vehicle to Police Headquarters.
- d. As prescribed in Department procedures 455.08(11) and 455.09 the vehicle should be processed and an Inventory Search conducted. Digital photographs of the vehicle shall also be taken to capture any existing damage.

7. **Release of Vehicle to Owner:** Section 460-83 A of the Town Code describes when an impounded vehicle may be released to the owner. In this context, in addition to the person in whose name the vehicle is registered means; the person who rented the vehicle as evidenced by the rental agreement, or a person authorized by the registered owner to be in possession of the vehicle as evidenced by a notarized letter from the registered owner indicating this. Under the law, a vehicle may be released to the owner:

- a. Upon payment of all towing, storage and administrative fees, and
- b. The owner or his/her agent posting cash security in an amount not to exceed the total of the maximum fines permitted upon conviction of the offenses charged in the outstanding summonses against the vehicle and the associated penalties levied because of the failure of the owner to timely answer; or
- c. The payment in full of all fines and associated penalties as well as towing, storage and administrative fees; and
- d. Presentation by the owner, or his agent of an order of the Court authorizing such release.

8. **Desk Officer Responsibility:** Section 460-83 B, C, delineates the responsibilities of supervisory personnel as they pertain to vehicles impounded under the Town's Scofflaw legislation. Under the law, supervisory police personnel are empowered to "determine the amount of security that the owner, operator or agent of the owner, must post for the release of the vehicle" and, "to establish a date in Greenburgh Town Court for the owners of any towed and impounded vehicle to answer outstanding parking summonses." When

a person authorized to claim a vehicle that has been impounded under the Town's Scofflaw Program comes to Police Headquarters to claim their vehicle, the Desk officer (assuming that the Desk officer is a supervisor) shall;

a. Ascertain the total amount of fines and penalties owed by the owner on tickets that remain unanswered for a minimum of forty-five (45) days. Although the Desk officer is not mandated to set security at the full amount of the outstanding fines and penalties, **DOING SO IS DESIRABLE AND SHOULD BE THE RULE RATHER THAN THE EXCEPTION** since the owner has obviously not answered the summonses received by the dates prescribed and has disregarded one or more notices routinely sent by Complus to such individuals as reminders. Moreover, the purpose of this law is to recover any fines and penalties that may ultimately be due the Town for summonses that have remained unanswered for protracted periods of time.

b. The amount of security set shall be paid in cash.

c. Cash received as security shall be handled in the same manner as cash bail. The person posting the security shall be provided with a receipt. As with cash bail, the person whose name appears on the receipt will be the one to whom the security is returned upon completion of Court proceedings. The receipt shall also indicate the Court Appearance date set by the supervisor.

d. Court Appearance Date - Since Scofflaws will be handled in Court on Wednesdays by the Town Attorney's office, the Supervisor shall make the return date a Wednesday providing at least **SEVEN (7)** days notice is given to allow the paperwork to be received and reviewed by the Town Attorney. The Supervisor will prepare and serve a **MUNICIPAL VIOLATION NOTICE** on the owner/agent indicating the return date and noting "**SCOFFLAW VIOLATION**" in the area of the Notice describing the violation. Return dates shall not be set on Wednesdays that fall on a holiday or on a Wednesday that the Town Attorney has indicated should not be used. In these situations, the next Wednesday when the Town Attorney is available should be used.

d. Upon the posting of security, and in addition to providing a receipt and Municipal Violation Notice to the owner/agent, the Supervisor accepting the security shall complete a **HOLD ON SCOFFLAW STATUS, UF 138** form. Preparation of this form will ensure that any vehicle released after security is posted will not erroneously be towed a second time. It will direct Court and Complus personnel to place a "Hold" on the Scofflaw Status of the vehicle in the database ensuring it will not be towed again for the same violation. Subsequent to each release, the Desk Officer or Police Supervisor setting and accepting security shall cause a copy of the completed UF 138 to be faxed to the Court at **682-5378**. Communications personnel shall enter their name and the date and time the UF 138 was faxed in the appropriate field on the UF 138. The original shall be forwarded to Records with the Scofflaw Paperwork.

NOTE

Although security may be accepted for an impounded vehicle on weekends and holidays, since Records is not open for business on these days the vehicle cannot be physically released until the next regular business day. Supervisory personnel may, none-the-less set and accept security as well as advise the owner of what additional steps must taken to secure the release of the vehicle.

e. People coming to Police Headquarters during times when the Court is open and who wish to pay their outstanding fines and penalties, may be directed to the Court.

NOTE

Court personnel are not empowered to accept security for the release of a vehicle. This responsibility lies exclusively with sworn Supervisory personnel. Therefore, the only way a vehicle impounded under this section can be released without first seeing a judge is for the owner to either pay their fines and penalties or post the amount of security set by a police supervisor as well as pay the tow bill, administrative and any storage fees.

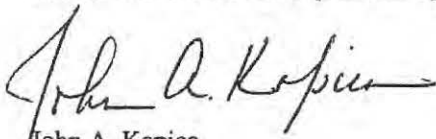
f. Once the requisite amount of security is posted and a receipt provided, the Desk officer shall direct the owner to the Records Unit for completion of the processing and release of the vehicle.

9. **Records Unit Personnel Responsibility:** Records Unit personnel shall be responsible for processing the release of all impounded vehicles. This shall include the following.

a. Upon receipt of paperwork indicating that the Department has impounded a vehicle under the Scofflaw Program, the Commanding Officer of the Records Unit shall first ensure that Records personnel forward a hard copy of the UF 138, Hold on Scofflaw Status form to the Court. A second hard copy of the UF 138 shall be included with the daily mailing of tickets to Complus.

b. That Commanding Officer of the Records Unit shall also ensure that a letter notifying the last registered owner that their vehicle has been impounded under the Scofflaw Program and what steps need to be taken to recover the vehicle is prepared and forwarded by certified mail, return receipt requested. Such letter shall be generated during the first business day after this information is received by the Records Unit.

c. The general procedures for the release of an impounded vehicle shall apply to the release of a vehicle impounded for violation of the Town's Scofflaw Program. Records unit personnel shall release a vehicle to the registered owner (agent or renter), upon production by that individual of a receipt for security issued by a supervisor in the Police Department or upon notice from the Court that the unanswered tickets upon which the vehicle has been declared a Scofflaw have been satisfied or answered and upon presentation of proof that the tow bill has been paid and upon payment of the administrative and storage fees.



John A. Kapica
Chief of Police



HOLD ON SCOFFLAW STATUS

This will certify that the following described vehicle was impounded under § 460-82 of the Greenburgh Code on _____ and that the owner/agent of the owner has posted \$ _____ in security against the amount indicated as being due in fines and penalties for the unanswered parking tickets and that a **"HOLD"** should now be placed against the Scofflaw Status of this vehicle to ensure that it is not subsequently impounded for the same violation. Please ensure that the database is updated to reflect a **"HOLD"** has been placed against the Scofflaw Status of this vehicle. The owner/agent of owner of the vehicle is scheduled to appear in Town Court on _____ to answer the outstanding parking tickets.

Vehicle Description:

Year: _____ Make: _____ Model: _____
Registration Number: _____ State: _____ Expiration: _____
Registered Owner: _____
Address: _____
City: _____ State: _____ Zip: _____

Fax To Court at 682-5378, Enter Date and Time Faxed and the Name and Computer ID# of Dispatcher

Supervisor's Signature and Computer ID#

Report Number

Records Personnel: Forward a hard copy of this form to the Town Court and to Complus.

UF 138 (10/09)

INV TOWN OF GREENBURGH 1
TO: PURCHASING
177 HILLSIDE AVE.
WHITE PLAINS NY 10603

PURCHASE ORDER No. 0020100366	
THIS PURCHASE ORDER CANNOT BE USED FOR ANY OTHER PURPOSES ALL TAXES ARE THE RESPONSIBILITY OF THE PURCHASER	
APPROPRIATIONS	AMOUNT
B.3120.250.0	19,707.00
TOTAL	19,707.00

PURCHASE ORDER

VENDOR

SHIP TO

866-967-4900
REMINGTON ELSAG LAW
ENFORCEMENT SYSTEM, LLC
870 REMINGTON DRIVE
MADISON NC 27025

TOWN OF GREENBURGH
POLICE DEPT.
ATTN: CAPT. WEISNER
188 TARRYTOWN ROAD

WHITE PLAINS, NEW YORK 10607

DATE	VENDOR	BID NO.	DEPT NO.	SHIP VIA	TERMS	REQUISITION NO.	
2/03/10	19767		B3120				
ITEM CODE	DESCRIPTION OF GOODS OR SERVICE			QUANTITY	U/M	UNIT PRICE	EXTENDED PRICE
MPH-900	RELES MPH-900X2AD3 MOBILE LICENSE PLATE reader with processor, enclosure with 2 cameras and infrared illuminators etc. and related software for above and permanent mount for cameras, includes installation			1.000	EA	16,800.00000	16,800.00
WARRANTY	WARRANTY COVERS ALL PARTS & LABOR for above equipment and software, onsite, for a period of 12 months after the existing warranty (12 months after receipt of equipment).			1.000	EA	1,600.00000	1,600.00
MPH 900 LIC.	OPERATIONS CENTER LICENSE			1.000	EA	972.00000	972.00
CAR KIT	ADDITIONAL CAR			1.000	EA	335.00000	335.00
						SUB TOTAL	
						FREIGHT CHG.	
OUR TAX EXEMPTION CERTIFICATE NO. 13-6007293						TOTAL	

CONDITIONS.

1. Municipality is exempt from payment of all Federal and New York State Taxes. Do not include taxes when submitting claim.
2. No charge shall be made by vendor for handling boxing, packing or transportation unless by prior written agreement.
3. Each box or package shall contain a memorandum showing contents, shipper's name and address, and purchase order number.
4. All goods received with subsequent privilege to inspect and return at vendor's expense, if defective or not in compliance with specifications.
5. The seller agrees to defend, save and hold harmless the Municipality, its Agents, Officials and Employees against any suit or damage claim or demand for actual or alleged infringement of any patent or patents by reason of the purchase and/or use of the articles hereby ordered.
6. This order may be cancelled by the purchasing clerk of the Municipality, if delivery is not made within a reasonable time.
7. Municipality is not responsible for purchases made except on written orders.
8. Notify at once of any changes in price as this order cannot be filled at higher price than last charged or quoted unless agreed by Municipality.
9. All bills must be rendered to Comptroller's Office, at Municipality, on claim for payment attached and certification must be signed by claimant.

APPROVAL OF FUNDS/PURCHASE AUTHORIZATION
I CERTIFY THAT THERE ARE MONIES AVAILABLE TO PAY THIS ORDER AND THE APPROPRIATION ACCOUNTS
HAVE BEEN ENCUMBERED FOR THE AMOUNT OF THE ORDER.

DIRECTOR OF PURCHASING

DATE

PURCHASING COPY

INV TOWN OF GREENBURGH 2
 TO: PURCHASING
 177 HILLSIDE AVE.
 WHITE PLAINS NY 10603

PURCHASE ORDER No. 0020100366	
THIS PURCHASE ORDER IS AN INSTRUMENT APPROVED BY THE TOWN OF GREENBURGH AND IS SUBJECT TO THE TOWN OF GREENBURGH'S FINANCIAL POLICY.	
APPROPRIATIONS	AMOUNT
B.3120.250.0	19,707.00
TOTAL	19,707.00

PURCHASE ORDER

VENDOR

SHIP TO

866-967-4800
 REMINGTON ELSAG LAW
 ENFORCEMENT SYSTEM, LLC
 870 REMINGTON DRIVE
 MADISON NC 27025

TOWN OF GREENBURGH
 POLICE DEPT.
 ATTN: CAPT. WEISNER
 188 TARRYTOWN ROAD

WHITE PLAINS, NEW YORK 10607

DATE	VENDOR	BID NO.	DEPT NO.	SHIP VIA	TERMS	REQUISITION NO.	
2/03/10	19767		B3120				
ITEM CODE	DESCRIPTION OF GOODS OR SERVICE			QUANTITY	U/M	UNIT PRICE	EXTENDED PRICE
	KIT WITH CABLES, gps with USB extension, software, and labor to install						
SUB TOTAL							
FREIGHT CHG.							
OUR TAX EXEMPTION CERTIFICATE NO. 13-6007293						TOTAL	19,707.00

CONDITIONS.

1. Municipality is exempt from payment of all Federal and New York State Taxes. Do not include taxes when submitting claim.
2. No charge shall be made by vendor for handling boxing, packing or transportation unless by prior written agreement.
3. Each box or package shall contain a memorandum showing contents, shipper's name and address, and purchase order number.
4. All goods received with subsequent privilege to inspect and return at vendor's expense, if defective or not in compliance with specifications.
5. The seller agrees to defend, save and hold harmless the Municipality, its Agents, Officers and Employees against any suit or damage claim or demand for actual or alleged infringement of any patent or patents by reason of the purchase and/or use of the articles hereby ordered.
6. This order may be cancelled by the purchasing clerk of the Municipality, if delivery is not made within a reasonable time.
7. Municipality is not responsible for purchases made except on written orders.
8. Notify at once of any changes in price as this order cannot be filled at higher price than last charged or quoted unless agreed by Municipality.
9. All bills must be rendered to Comptroller's Office, at Municipality, on claim for payment attached and certification must be signed by claimant.

APPROVAL OF FUNDS/PURCHASE AUTHORIZATION

I CERTIFY THAT THERE ARE MONIES AVAILABLE TO PAY THIS ORDER AND THE APPROPRIATION ACCOUNTS HAVE BEEN ENCUMBERED FOR THE AMOUNT OF THE ORDER.

DIRECTOR OF PURCHASING

DATE

PURCHASING COPY

TO: TOWN OF GREENBURGH
 177 HILLSIDE AVENUE
 WHITE PLAINS NY 10603

PURCHASE ORDER No. 0020072195	
THIS PURCHASE ORDER NUMBER MUST APPEAR ON ALL PACKAGES, INVOICES AND CORRESPONDENCE	
R.3120.250.0	17,955.00

PURCHASE ORDER

VENDOR
 REMINGTON ELSAG LAW
 ENFORCEMENT SYSTEM, LLC
 970 REMINGTON DRIVE
 MADISON NC 27025

SHIP TO
 TOWN OF GREENBURGH
 POLICE DEPT.
 ATTN: CAPT. WEISNER
 189 TARRYTOWN ROAD
 WHITE PLAINS, NEW YORK 10607

6/04/07	19767	93120				
ITEM CODE	DESCRIPTION OF GOODS OR SERVICES	QUANTITY	U/M	UNIT PRICE	EXTENDED PRICE	
MPH-900	RELES MPH-900 MOBILE LICENSE PLATE READER WITH PROCESSOR, ENCLOSURE WITH 2 CAMERAS AND INFRARED ILLUMINATORS ETC. AND RELATED SOFTWARE FOR ABOVE AND PERMANENT MOUNT FOR CAMERAS	1.000	EA	16,800.00000	16,800.00	
INSTALL	INSTALLATION OF PERMANENT MOUNTS FOR CAMERAS	1.000	EA	300.00000	300.00	
WARRANTY	WARRANTY COVERS ALL PARTS & LABOR FOR ABOVE EQUIPMENT AND SOFTWARE, ONSITE, FOR A PERIOD OF 12 MONTHS AFTER THE EXISTING WARRANTY (12 MONTHS AFTER RECEIPT OF EQUIPMENT). EXTENDED WARRANTY COVERS UPDATES AND IS RENEWABLE AT 5% OF EQUIPMENT COST	1.000	EA	355.00000	355.00	
				SUB TOTAL		
				FREIGHT CHG.		
OUR TAX EXEMPTION CERTIFICATE NO. 13 - 6007293				TOTAL		
CONDITIONS 1. Municipality is exempt from payment of all Federal and New York State Taxes. Do not include taxes when submitting claim. 2. No charge shall be made by vendor for handling, boxing, packing or transportation unless by prior written agreement. 3. Each box or package shall contain a memorandum showing contents, shipper's name and address, and purchase order number. 4. All goods received with subsequent privilege to inspect and return at vendor's expense if defective or not in compliance with specifications. 5. The seller agrees to defend, save and hold harmless the Municipality, its Agents, Officials and Employees against any suit or damage claim or demand for actual or alleged infringement of any patent or patents by reason of the purchase and/or use of the articles hereby ordered. 6. This order may be cancelled by the purchasing clerk of the Municipality if delivery is not made within a reasonable time. 7. Municipality is not responsible for purchases made except on written orders. 8. Notify at once of any changes in price as this order cannot be filled at higher price than last charged or quoted unless agreed by Municipality. 9. All bills must be rendered to Comptroller's Office, at Municipality, on claim for payment attached and certification must be signed by claimant.						

APPROVAL OF FUNDS/PURCHASE AUTHORIZATION

I CERTIFY THAT THERE ARE MONEYS AVAILABLE TO PAY THIS ORDER AND THE APPROPRIATION ACCOUNTS HAVE BEEN ENCUMBERED FOR THE AMOUNT OF THE ORDER.

DIRECTOR OF PURCHASING

DATE

PURCHASING COPY

TO: TOWN OF GREENBURGH 2
177 HILLSIDE AVENUE
WHITE PLAINS NY 10603

PURCHASE ORDER No. 0020072195	
THIS PURCHASE ORDER NUMBER MUST APPEAR ON ALL PACKAGES, INVOICES AND CORRESPONDENCE	
8.3120.250.0	17,955.00

PURCHASE ORDER

VENDOR

REMINGTON ELSAG LAW
ENFORCEMENT SYSTEM, LLC
370 REMINGTON DRIVE
MADISON NC 27025

SHIP TO

TOWN OF GREENBURGH
POLICE DEPT.
ATTN: CAPT. WEISNER
188 TARRYTOWN ROAD

WHITE PLAINS, NEW YORK 10607

8/04/07	19767	83120				
ITEM CODE	DESCRIPTION OF GOODS OR SERVICES	QUANTITY	U/M	UNIT PRICE	EXTENDED PRICE	
PC-62117	PER YEAR. AS PER NYS CONTRACT #PC62117	1.000	EA			
				SUB TOTAL		
				FREIGHT CHG.		
OUR TAX EXEMPTION CERTIFICATE NO. 13 - 8007293				TOTAL	17,955.00	
CONDITIONS 1. Municipality is exempt from payment of all Federal and New York State Taxes. Do not include taxes when submitting claim. 2. No charge shall be made by vendor for handling, boxing, packing or transportation unless by prior written agreement. 3. Each box or package shall contain a memorandum showing contents, shipper's name and address, and purchase order number. 4. All goods received with subsequent privilege to inspect and return at vendor's expense if defective or not in compliance with specifications. 5. The seller agrees to defend, save and hold harmless the Municipality, its Agents, Officials and Employees against any suit or damage claim or demand for actual or alleged infringement of any patent or patents by reason of the purchase and/or use of the articles hereby ordered. 6. This order may be canceled by the purchasing clerk of the Municipality if delivery is not made within a reasonable time. 7. Municipality is not responsible for purchases made except on written orders. 8. Notify at once of any changes in price as this order cannot be filled at higher price than last charged or quoted unless agreed by Municipality. 9. All bills must be rendered to Comptroller's Office, at Municipality, on claim for payment attached and certification must be signed by claimant.						

APPROVAL OF FUNDS/PURCHASE AUTHORIZATION

I CERTIFY THAT THERE ARE MONEYS AVAILABLE TO PAY THIS ORDER AND THE APPROPRIATION ACCOUNTS HAVE BEEN ENCUMBERED FOR THE AMOUNT OF THE ORDER.

DIRECTOR OF PURCHASING

DATE

PURCHASING COPY



STATE OF NEW YORK
DIVISION OF CRIMINAL JUSTICE SERVICES
4 Tower Place
Albany, New York 12203-3764
<http://criminaljustice.ny.gov>

ANDREW M. CUOMO
GOVERNOR

MICHAEL C. GREEN
EXECUTIVE DEPUTY COMMISSIONER

July 20, 2012

Greenburgh Town Police Department
Chief Joseph DeCarlo
188 Tarrytown Rd
White Plains, NY 10607-1624

Dear Chief DeCarlo:

Thank you for your execution of the Use and Dissemination Agreement between our respective agencies. The Division of Criminal Justice Services (DCJS) will retain one copy and the other copy is enclosed for your files.

As always, should you have any questions related to your Use and Dissemination Agreement, please contact the DCJS Customer Contact Center at 1-800-262-3257 and ask to be directed to the U&D group for assistance.

Sincerely,

Ann Sammons
Chief of Operations
Office of Criminal Justice Operations

Enclosure

-1-
USE & DISSEMINATION AGREEMENT
between
NEW YORK STATE DIVISION OF CRIMINAL JUSTICE SERVICES
and
Greenburgh Town Police Department

Pursuant to Executive Law §837(6) and §837(8-a), the New York State Division of Criminal Justice Services (DCJS) hereby agrees to allow **Greenburgh Town Police Department, White Plains, 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.

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.

PURGE/VALIDATION OF INACTIVE NON-CRIMINAL FINGERPRINT CARDS

If DCJS retains the User Agency's non-criminal applicant fingerprint cards in its files for the purpose of issuing reports to the User Agency upon the subsequent arrest of the subjects of the retained fingerprint cards, the User Agency agrees to:

At the end of every calendar year, provide DCJS with:

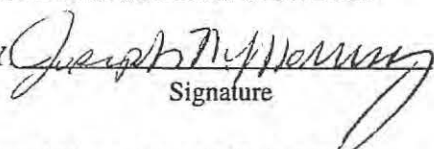
- 1) The names and NYSID numbers of individuals whose fingerprint cards were sent to DCJS for identification processing and retention, but whose applications were not approved for employment or licensure by the User Agency; and
- 2) The names and NYSID numbers of individuals who subsequently left the employment situation or relinquished the licensure.

Once so notified by the User Agency, DCJS agrees to purge the fingerprints of individuals who are no longer in the employment or licensure situation for which they were fingerprinted.

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

BY: 

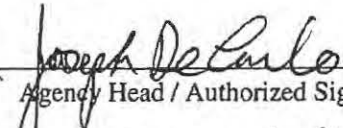
Signature

Printed Name: Joseph N. Morrissey

Title: Director
Office of Criminal Justice Operations

Date: 7-19-12

USER AGENCY: Greenburgh Town Police Dept.

BY: 

Agency Head / Authorized Signature

Printed Name: Joseph DeCarlo

Title: Chief of Police

Date: July 18, 2012

APPENDIX B

GUIDELINES FOR ELECTRONIC ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Employees who electronically access computer systems and the available information databases are the most important link in system security. Regardless of how well managers plan and document security rules and guidelines, it is the employee who directly accesses a computer system who must adhere to and work with the security rules and guidelines. Each employee with access to a computer system should have a thorough understanding of his/her responsibilities in accessing and disseminating information, recording transactions, and disposing of data printouts. Each employee should have access to written procedures on the subject of data security, including those issued by all State agencies that make information available through DCJS. If an employee is unsure of any of his/her legal responsibilities in these areas, a supervisor should be contacted immediately for assistance.

Operator Identification/Authorization:

DCJS maintains a list of individuals who are authorized to access criminal history record information as part of their work duties (Users). Each User is assigned a unique and secret Password which he/she must use at logon to authenticate the User. Once authenticated, a session is established and a User log is automatically maintained by the system to establish a record of who transacted each inquiry. Because the User is responsible for all inquiries made during that session, the terminal should not be left unattended once the User has logged on. The User should not inform anyone else of his/her Password, or use another person's Usercode and Password. Under no circumstances should a list of Users and Passwords be written or posted where anyone may see them, such as near the terminal or in written procedures. Passwords should be changed regularly or whenever the User feels his/her Password has been compromised.

Supporting Documentation/Audits:

DCJS, as the manager of electronic software services, will conduct routine periodic audits of a User Agency to ensure compliance with relevant State and Federal confidentiality policies, and all applicable State and Federal laws. An audit may also be conducted if there is reason to suspect that a security violation may have been committed or attempted. As part of DCJS auditing requirements, a User Agency will be required to run a monthly utility program which will provide a log of all criminal history record transactions. It will be the responsibility of the User Agency's Terminal Agency Coordinator to review this log and validate the fact that usage was for official purposes and consistent with DCJS policy. The results of this review must be available to the DCJS Audit Unit on request and in the manner and form in which requested.

Failure to Adhere to Law and Regulations:

DCJS may conduct an audit when a breach of security is suspected or reported. Repeated and/or serious violations may result in suspension of service and the imposition of fines.

Appendix C

28 CFR PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS (current as of 11/30/11)

Subpart A—General Provisions

- § 20.1 Purpose.
- § 20.2 Authority.
- § 20.3 Definitions.

Subpart B—State and Local Criminal History Record Information Systems

- § 20.20 Applicability.
- § 20.21 Preparation and submission of a Criminal History Record Information Plan.
- § 20.22 Certification of compliance.
- § 20.23 Documentation: Approval by OJARS.
- § 20.24 State laws on privacy and security.
- § 20.25 Penalties.

Subpart C—Federal Systems and Exchange of Criminal History Record Information

- § 20.30 Applicability.
 - § 20.31 Responsibilities.
 - § 20.32 Includable offenses.
 - § 20.33 Dissemination of criminal history record information.
 - § 20.34 Individual's right to access criminal history record information.
 - § 20.35 Criminal Justice Information Services Advisory Policy Board.
 - § 20.36 Participation in the Interstate Identification Index System.
 - § 20.37 Responsibility for accuracy, completeness, currency, and integrity.
 - § 20.38 Sanction for noncompliance.
- Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems

Authority: 28 U.S.C. 534; Pub. L. 92–544, 86 Stat. 1115; 42 U.S.C. 3711, *et seq.*, Pub. L. 99–169, 99 Stat. 1002, 1008–1011, as amended by Pub. L. 99–569, 100 Stat. 3190, 3196; Pub. L. 101–515, as amended by Pub. L. 104–99, set out in the notes to 28 U.S.C. 534.

Source: Order No. 601–75, 40 FR 22114, May 20, 1975, unless otherwise noted.

Subpart A—General Provisions

Source: 41 FR 11714, Mar. 19, 1976, unless otherwise noted.

§ 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

[Order No. 2258–99, 64 FR 52226; Sept. 28, 1999]

§ 20.2 Authority.

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Public Law 93–83, 87 Stat. 197, 42 U.S.C. 3701, *et seq.* (Act), 28 U.S.C. 534, and Public Law 92–544, 86 Stat. 1115.

§ 20.3 Definitions.

Appendix C

As used in these regulations:

(a) *Act* means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701, *et seq.*, as amended.

(b) *Administration of criminal justice* means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(c) *Control Terminal Agency* means a duly authorized state, foreign, or international criminal justice agency with direct access to the National Crime Information Center telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

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

(e) *Criminal history record information system* means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of criminal history record information.

(f) *Criminal history record repository* means the state agency designated by the governor or other appropriate executive official or the legislature to perform centralized recordkeeping functions for criminal history records and services in the state.

(g) *Criminal justice agency* means:

(1) Courts; and

(2) A 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. State and federal Inspector General Offices are included.

(h) *Direct access* means having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

(i) *Disposition* means information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(j) *Executive order* means an order of the President of the United States or the Chief Executive of a state that has the force of law and that is published in a manner permitting regular public access.

(k) *Federal Service Coordinator* means a non-Control Terminal Agency that has a direct telecommunications line to the National Crime Information Center network.

Appendix C

(l) *Fingerprint Identification Records System* or "FIRS" means the following FBI records: Criminal fingerprints and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities; civil fingerprints submitted by federal agencies and civil fingerprints submitted by persons desiring to have their fingerprints placed on record for personal identification purposes; identification records, sometimes referred to as "rap sheets," which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the FIRS; and a name index pertaining to all individuals whose fingerprints are maintained in the FIRS. See the FIRS Privacy Act System Notice periodically published in the Federal Register for further details.

(m) *Interstate Identification Index System* or "III System" means the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

(n) *National Crime Information Center* or "NCIC" means the computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The NCIC includes, but is not limited to, information in the III System. See the NCIC Privacy Act System Notice periodically published in the Federal Register for further details.

(o) *National Fingerprint File* or "NFF" means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(p) *National Identification Index* or "NII" means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(q) *Nonconviction data* means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; information disclosing that the police have elected not to refer a matter to a prosecutor, that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed; and information that there has been an acquittal or a dismissal.

(r) *State* means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(s) *Statute* means an Act of Congress or of a state legislature or a provision of the Constitution of the United States or of a state.

[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

Subpart B—State and Local Criminal History Record Information Systems

Source: 41 FR 11715, Mar. 19, 1976, unless otherwise noted.

§ 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to title I of the Act. Use of information obtained from the FBI Identification Division or the FBI/NCIC system shall also be subject to limitations contained in subpart C.

(b) The regulations in this subpart shall not apply to criminal history record information contained in:

(1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

Appendix C

(2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis;

(3) Court records of public judicial proceedings;

(4) Published court or administrative opinions or public judicial, administrative or legislative proceedings;

(5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses;

(6) Announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

§ 20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to OJARS by each State on March 16, 1976, to set forth all operational procedures, except those portions relating to dissemination and security. A supplemental plan covering these portions shall be submitted no later than 90 days after promulgation of these amended regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.* Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information unless it can be assured that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period.

(2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.* Insure that dissemination of nonconviction data has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, as construed by appropriate State or local officials or agencies;

Appendix C

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section 524(a), and provide sanctions for the violation thereof. These dissemination limitations do not apply to conviction data.

(c) *General policies on use and dissemination.* (1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given.

(2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.

(3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

(d) *Juvenile records.* Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute, court order, rule or court decision specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in paragraph (b) (3) and (4) of this section.

(e) *Audit.* Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

(f) *Security.* Wherever criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(i) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(a) Criminal history record information is stored by the computer in such manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(b) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(c) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

Appendix C

(d) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(e) The programs specified in paragraphs (f)(3)(i) (b) and (d) of this section are known only to criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(f) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for (1) the physical security of criminal history record information under its control or in its custody and (2) the protection of such information from unauthorized access, disclosure or dissemination.

(g) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(ii) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(i) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(ii) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(iii) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for

(a) The physical security of criminal history record information under its control or in its custody and

(b) The protection of such information from unauthorized access, disclosure, or dissemination.

(iv) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(v) Provide that direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

(g) *Access and review.* Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

Appendix C

- (3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;
- (4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;
- (5) The correcting agency shall notify all criminal justice recipients of corrected information; and
- (6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by §20.3(b).

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61595, Dec. 6, 1977]

§ 20.22 Certification of compliance.

(a) Each State to which these regulations are applicable shall with the submission of its plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

- (1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under §20.21(g) must be completely operational;
- (2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;
- (3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;
- (4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and
- (5) A listing setting forth categories of non-criminal justice dissemination. See §20.21(b).

§ 20.23 Documentation: Approval by OJARS.

Within 90 days of the receipt of the plan, OJARS shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by OJARS will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by March 1, 1978. A final certification shall be submitted on March 1, 1978.

Where a State finds it is unable to provide final certification that all required procedures as set forth in §20.21 will be operational by March 1, 1978, a further extension of the deadline will be granted by OJARS upon a showing that the State has made a good faith effort to implement these regulations to the maximum extent feasible. Documentation justifying the request for the extension including a proposed timetable for full compliance must be submitted to OJARS by March 1, 1978. Where a State submits a request for an extension, the implementation date will be extended an additional 90 days while OJARS reviews the documentation for approval or disapproval. To be approved, such revised schedule must be consistent with the timetable and procedures set out below:

- (a) July 31, 1978—Submission of certificate of compliance with:

Appendix C

- (1) Individual access, challenge, and review requirements;
- (2) Administrative security;
- (3) Physical security to the maximum extent feasible.

(b) Thirty days after the end of a State's next legislative session—Submission to OJARS of a description of State policy on dissemination of criminal history record information.

(c) Six months after the end of a State's legislative session—Submission to OJARS of a brief and concise description of standards and operating procedures to be followed by all criminal justice agencies covered by OJARS regulations in complying with the State policy on dissemination.

(d) Eighteen months after the end of a State's legislative session—Submission to OJARS of a certificate attesting to the conduct of an audit of the State central repository and of a random number of other criminal justice agencies in compliance with OJARS regulations.

[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61596, Dec. 6, 1977]

§ 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a civil penalty not to exceed \$10,000 for a violation occurring before September 29, 1999, and not to exceed \$11,000 for a violation occurring on or after September 29, 1999. In addition, OJARS may initiate fund cut-off procedures against recipients of OJARS assistance.

[41 FR 11715, Mar. 19, 1976, as amended by Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]

Subpart C—Federal Systems and Exchange of Criminal History Record Information

Source: Order No. 2258-99, 64 FR 52227, Sept. 28, 1999, unless otherwise noted.

§ 20.30 Applicability.

The provisions of this subpart of the regulations apply to the IJI System and the FIRS, and to duly authorized local, state, tribal, federal, foreign, and international criminal justice agencies to the extent that they utilize the services of the IJI System or the FIRS. This subpart is applicable to both manual and automated criminal history records.

§ 20.31 Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall manage the NCIC.

(b) The FBI shall manage the FIRS to support identification and criminal history record information functions for local, state, tribal, and federal criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by federal statute, state statute pursuant to Public Law 92-544, 86 Stat. 1115, Presidential executive order, or regulation or order of the Attorney General of the United States.

(c) The FBI CJIS Division may manage or utilize additional telecommunication facilities for the exchange of fingerprints, criminal history record related information, and other criminal justice information.

Appendix C

(d) The FBI CJIS Division shall maintain the master fingerprint files on all offenders included in the III System and the FIRS for the purposes of determining first offender status; to identify those offenders who are unknown in states where they become criminally active but are known in other states through prior criminal history records; and to provide identification assistance in disasters and for other humanitarian purposes.

(e) The FBI may routinely establish and collect fees for noncriminal justice fingerprint-based and other identification services as authorized by Federal law. These fees apply to Federal, State and any other authorized entities requesting fingerprint identification records and name checks for noncriminal justice purposes.

(1) The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records and name checks for noncriminal justice purposes.

(2) Fee amounts and any revisions thereto shall be determined by current costs, using a method of analysis consistent with widely accepted accounting principles and practices, and calculated in accordance with the provisions of 31 U.S.C. 9701 and other Federal law as applicable.

(3) Fee amounts and any revisions thereto shall be published as a notice in the Federal Register.

(f) The FBI will collect a fee for providing noncriminal name-based background checks of the FBI Central Records System through the National Name Check Program pursuant to the authority in Pub. L. 101-515 and in accordance with paragraphs (e)(1), (2) and (3) of this section.

[41 FR 11715, Mar. 19, 1976, as amended at 75 FR 18755, Apr. 13, 2010; 75 FR 24798, May 6, 2010]

§ 20.32 Includable offenses.

(a) Criminal history record information maintained in the III System and the FIRS shall include serious and/or significant adult and juvenile offenses.

(b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a §20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal history record repositories, including those states participating in the NFF.

(c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in the III System and the FIRS may be made available:

(1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;

(2) To federal agencies authorized to receive it pursuant to federal statute or Executive order;

(3) For use in connection with licensing or employment, pursuant to Public Law 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law. Refer to §50.12 of this chapter for dissemination guidelines relating to requests processed under this paragraph;

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses;

Appendix C

(5) To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);

(6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/ information services for criminal justice agencies; and

(7) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or service providers identified in paragraphs (a)(6) and (a)(7) of this section.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

(d) Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

§ 20.34 Individual's right to access criminal history record information.

The procedures by which an individual may obtain a copy of his or her identification record from the FBI to review and request any change, correction, or update are set forth in §§16.30–16.34 of this chapter. The procedures by which an individual may obtain a copy of his or her identification record from a state or local criminal justice agency are set forth in §20.34 of the appendix to this part.

§ 20.35 Criminal Justice Information Services Advisory Policy Board.

(a) There is established a CJIS Advisory Policy Board, the purpose of which is to recommend to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.

(b) The Board includes representatives from state and local criminal justice agencies; members of the judicial, prosecutorial, and correctional segments of the criminal justice community; a representative of federal agencies participating in the CJIS systems; and representatives of criminal justice professional associations.

(c) All members of the Board will be appointed by the FBI Director.

(d) The Board functions solely as an advisory body in compliance with the provisions of the Federal Advisory Committee Act, Title 5, United States Code, Appendix 2.

§ 20.36 Participation in the Interstate Identification Index System.

(a) In order to acquire and retain direct access to the III System, each Control Terminal Agency and Federal Service Coordinator shall execute a CJIS User Agreement (or its functional equivalent) with the Assistant Director in Charge of the CJIS Division, FBI, to abide by all present rules, policies, and procedures of the NCIC, as well as any rules, policies, and procedures hereinafter recommended by the CJIS Advisory Policy Board and adopted by the FBI Director.

Appendix C

(b) Entry or updating of criminal history record information in the III System will be accepted only from state or federal agencies authorized by the FBI. Terminal devices in other agencies will be limited to inquiries.

§ 20.37 Responsibility for accuracy, completeness, currency, and integrity.

It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

§ 20.38 Sanction for noncompliance.

Access to systems managed or maintained by the FBI is subject to cancellation in regard to any agency or entity that fails to comply with the provisions of subpart C of this part.

Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems

Subpart A—§20.3(d). The definition of criminal history record information is intended to include the basic offender-based transaction statistics/III System (OBTS/III) data elements. If notations of an arrest, disposition, or other formal criminal justice transaction occurs in records other than the traditional "rap sheet," such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g., suspected criminal activity, associates, hangouts, financial information, and ownership of property and vehicles) is not included in the definition of criminal history information.

§20.3(g). The definitions of criminal justice agency and administration of criminal justice in §20.3(b) of this part must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies, as well as subunits of noncriminal justice agencies that perform the administration of criminal justice pursuant to a federal or state statute or executive order and allocate a substantial portion of their budgets to the administration of criminal justice. The above subunits of noncriminal justice agencies would include, for example, the Office of Investigation of the Food and Drug Administration, which has as its principal function the detection and apprehension of persons violating criminal provisions of the Federal Food, Drug and Cosmetic Act. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services, such as New York's Division of Criminal Justice Services.

§20.3(i). Disposition is a key concept in section 524(b) of the Act and in §§20.21(a)(1) and 20.21(b) of this part. It therefore is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other, unspecified transactions concluding criminal proceedings within a particular agency.

§20.3(q). The different kinds of acquittals and dismissals delineated in §20.3(i) are all considered examples of nonconviction data.

Subpart B—§20.20(a). These regulations apply to criminal justice agencies receiving funds under the Omnibus Crime Control and Safe Streets Act for manual or automated systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulation of manual systems, therefore, is authorized by section 524(b) when coupled with section 501 of the Act which authorizes the Administration to establish rules and regulations "necessary to the exercise of its functions

* * *

Appendix C

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

Limitations as contained in subpart C also apply to information obtained from the FBI Identification Division or the FBI/NCIC System.

§20.20 (b) and (c). Section 20.20 (b) and (c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know. Court records of public judicial proceedings are also exempt from the provisions of the regulations.

Section 20.20(b)(2) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1975" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal justice agency may respond to the inquiry. Conviction data as stated in §20.21(b) may be disseminated without limitation.

§20.21. The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor. The State has 90 days from the publication of these revised regulations to submit the portion of the plan covering §§20.21(b) and 20.21(f).

§20.21(a)(1). Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to a statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.20(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repository.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

Appendix C

§20.21(b). The limitations on dissemination in this subsection are essential to fulfill the mandate of section 524(b) of the Act which requires the Administration to assure that the "privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

The regulations distinguish between conviction and nonconviction information insofar as dissemination is concerned. Conviction information is currently made available without limitation in many jurisdictions. Under these regulations, conviction data and pending charges could continue to be disseminated routinely. No statute, ordinance, executive order, or court rule is necessary in order to authorize dissemination of conviction data. However, nothing in the regulations shall be construed to negate a State law limiting such dissemination.

After December 31, 1977, dissemination of nonconviction data would be allowed, if authorized by a statute, ordinance, executive order, or court rule, decision, or order. The December 31, 1977, deadline allows the States time to review and determine the kinds of dissemination for non-criminal justice purposes to be authorized. When a State enacts comprehensive legislation in this area, such legislation will govern dissemination by local jurisdictions within the State. It is possible for a public record law which has been construed by the State to authorize access to the public of all State records, including criminal history record information, to be considered as statutory authority under this subsection. Federal legislation and executive orders can also authorize dissemination and would be relevant authority.

For example, Civil Service suitability investigations are conducted under Executive Order 10450. This is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquiries to appropriate law enforcement agencies.

§20.21(b)(3). This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§20.21(b)(4). Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in §20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

"Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations, pursuant to section 524(a) as soon as possible.

§20.21(c)(2). Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§20.21(c)(3). The language of this subsection leaves to the States the question of who among the agencies and individuals listed in §20.21(b) shall actually receive criminal records. Under these regulations a State could place a

Appendix C

total ban on dissemination if it so wished. The State could, on the other hand, enact laws authorizing any member of the private sector to have access to non-conviction data.

§20.21(d). Non-criminal justice agencies will not be able to receive records of juveniles unless the language of a statute or court order, rule, or court decision specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§20.21(e) Since it would be too costly to audit each criminal justice agency in most States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies. Although this subsection requires that there be records kept with the names of all persons or agencies to whom information is disseminated, criminal justice agencies are not required to maintain dissemination logs for "no record" responses.

§20.21(f). Requirements are set forth which the States must meet in order to assure that criminal history record information is adequately protected. Automated systems may operate in shared environments and the regulations require certain minimum assurances.

§20.21(g)(1). A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that States ought to be free to determine other means of identity verification.

§20.21(g)(5). Not every agency will have done this in the past, but henceforth adequate records including those required under 20.21(e) must be kept so that notification can be made.

§20.21(g)(6). This section emphasizes that the right to access and review extends only to criminal history record information and does not include other information such as intelligence or treatment data.

§20.22(a). The purpose for the certification requirement is to indicate the extent of compliance with these regulations. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

Note: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Reports No. 2 and No. 13; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum No. 3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum No. 4.

Subpart C—§20.31. This section defines the criminal history record information system managed by the Federal Bureau of Investigation. Each state having a record in the III System must have fingerprints on file in the FBI CJIS Division to support the III System record concerning the individual.

Paragraph (b) is not intended to limit the identification services presently performed by the FBI for local, state, tribal, and federal agencies.

§20.32. The grandfather clause contained in paragraph (c) of this section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses that were stored prior to February, 1973. In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will also appear in the arrest segment of the III System record.

Appendix C

§20.33(a)(3). This paragraph incorporates provisions cited in 28 CFR 50.12 regarding dissemination of identification records outside the federal government for noncriminal justice purposes.

§20.33(a)(6). Noncriminal justice governmental agencies are sometimes tasked to perform criminal justice dispatching functions or data processing/information services for criminal justice agencies as part, albeit not a principal part, of their responsibilities. Although such inter-governmental delegated tasks involve the administration of criminal justice, performance of those tasks does not convert an otherwise non-criminal justice agency to a criminal justice agency. This regulation authorizes this type of delegation if it is effected pursuant to executive order, statute, regulation, or interagency agreement. In this context, the noncriminal justice agency is servicing the criminal justice agency by performing an administration of criminal justice function and is permitted access to criminal history record information to accomplish that limited function. An example of such delegation would be the Pennsylvania Department of Administration's Bureau of Consolidated Computer Services, which performs data processing for several state agencies, including the Pennsylvania State Police. Privatization of the data processing/information services or dispatching function by the noncriminal justice governmental agency can be accomplished pursuant to §20.33(a)(7) of this part.

§20.34. The procedures by which an individual may obtain a copy of his manual identification record are set forth in 28 CFR 16.30–16.34.

The procedures by which an individual may obtain a copy of his III System record are as follows: If an individual has a criminal record supported by fingerprints and that record has been entered in the III System, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

Procedure. 1. All requests for review must be made by the subject of the record through a law enforcement agency which has access to the III System. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry through NCIC to obtain his III System record or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Clarksburg, West Virginia, by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI, or, possibly, in the state's central identification agency.

4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§20.36. This section refers to the requirements for obtaining direct access to the III System.

§20.37. The 120-day requirement in this section allows 30 days more than the similar provision in subpart B in order to allow for processing time that may be needed by the states before forwarding the disposition to the FBI.

[Order No. 662–76, 41 FR 34949, Aug. 18, 1976, as amended by Order No. 1438–90, 55 FR 32075, Aug. 7, 1990; Order No. 2258–99, 64 FR 52229, Sept. 28, 1999]



MEMORANDUM OF AGREEMENT FOR THE WESTCHESTER INTELLIGENCE CENTER (WIC) AMONG THE PARTICIPATING FEDERAL, STATE AND LOCAL LAW ENFORCEMENT AGENCIES

1. Overview

a. Background:

The Westchester Intelligence Center ("WIC") was established as a crime intelligence center to foster and facilitate information sharing and collaboration among law enforcement agencies, particularly field intelligence officers, operating in Westchester County as a means of increasing the ability of law enforcement to rapidly triage criminal events that endanger public safety and quickly respond to situations as they develop.

The principal goal of WIC is to support local police agencies in their efforts to abate crime and augment public safety in Westchester County.

WIC operates under the auspices of the Westchester County District Attorney's Office ("WCDAO") and is staffed by members of multiple law enforcement agencies. WIC is headed by an Executive Director, who shall serve as the Administrator of this Agreement ("Administrator").

b. Purpose and Intended Benefits:

With the goal of enhancing public safety, while protecting individual privacy rights, the parties to this agreement seek to establish a mechanism for the sharing and exchange of criminal intelligence information and data for the advancement of legitimate law enforcement purposes, including crime solving and abatement, identification and location of suspects and known offenders, detection of predictive trends in criminal activity, and development of strategies to solve and prevent crimes.

c. Agency Participation:

Any federal, state or local law enforcement agency operating in Westchester County ("Agency") may participate in WIC.

2. Information and Resources to be Shared:

Subject to the confidentiality provisions outlined in this agreement, WCDAO will make the resources of WIC available to all participating Agencies. WIC will share information

and data – whether generated by WIC or provided to WIC by outside law enforcement agencies - with participating Agencies for legitimate law enforcement purposes only.

3. Requests for Information:

All requests for information and data from WIC shall be submitted to the Administrator or his/her designated representative. The Administrator shall be the final arbiter of whether the information and data requested by the Agency is available for dissemination.

4. Record Retention:

It is understood and agreed that the requesting Agency is responsible for the preservation of all records and/or reports generated by WIC at the request of the Agency, and shall be the repository of those records and reports.

Each Agency shall retain, as part of its own case files and records, any records and reports (electronic and physical copies) obtained from WIC. The retention shall be in accordance with that Agency's policies for record retention and in compliance with any and all applicable federal, state, county and local laws.

5. Confidentiality and Security:

- In accordance with its purpose WIC shall be permitted to disseminate information and data supplied by an Agency to authorized users under the terms provided herein except to the extent such information and data has been specifically identified as "confidential" by the providing agency.
- Information and data possessed by WIC is subject to disclosure in accordance with the laws governing the criminal justice system and by court order.
- Only authorized users are allowed to view and use the information and data possessed by WIC. Any authorized user who receives a request from a non-authorized user for information and data provided by WIC shall not release that information, but may refer the requestor to the Administrator.
- Each Agency will make reasonable arrangements to maintain the security of the information and data in its custody, by protecting it against such risks as unauthorized access, collection, use, disclosure or disposal.
- Each Agency will advise WCDAB and WIC immediately of any circumstances, incidents or events concerning the following: unauthorized access to or modification of information or data supplied by WIC; unauthorized use of such information and data; unauthorized disclosure of such information and data; and breaches of privacy, security and confidentiality with respect to the information and data or with respect to any computer system in its custody that is used to store or access such information and data.
- Each Agency must investigate and cure any of the aforementioned incidents of unauthorized use of WIC information and/or data.

- All employees of WIC and each participating Agency having access to information and data stored and maintained at WIC will be subject to a criminal investigation background check.
- Each Agency will inform the Administrator or his/her designee, in writing, when an employee or agent of the Agency is no longer authorized to access WIC as a representative of the Agency.

6. Third Party Dissemination of Information and Data:

There shall be no third-party dissemination by an Agency of information and data obtained through WIC without the express, written consent of the Administrator.

7. Accuracy:

Each Agency will make every reasonable effort to ensure the information and data it contributes to WIC is accurate, complete and up-to-date.

It is expressly understood and agreed that an Agency shall use the ordinary investigative tools to insure the objective reliability of any information and data received from WIC which is relied upon to conduct any police initiated encounters.

8. Modification or Termination – General:

This agreement may be modified or terminated at any time by agreement, in writing, of both parties.

9. Termination for Non-Compliance:

This agreement may be terminated at any time by either Party if the other Party fails to meet its obligations under this agreement.

It is expressly understood and agreed that this agreement will, at the election of the Administrator, cease immediately if a recipient Agency is found to be improperly using or disclosing the shared information and data. In addition, such improper use or disclosure will be subject to the penalties provided by applicable law.

10. Term of Agreement:

This agreement shall go into effect upon full execution hereof by both parties. It shall remain in effect unless and until terminated in accordance with paragraph 8 or 9.

11. Notices:

Any notices required by this agreement shall be in writing and shall be effective on mailing. All notices shall be sent by registered or certified mail, return receipt requested, or by overnight courier, and mailed to the following addresses:

WCDA: Honorable Janet DiFiore
District Attorney of Westchester County
Westchester County Courthouse
111 Dr. Martin Luther King, Jr. Blvd.
White Plains, New York 10601

With copy to: Robert Kelly
Executive Director
Westchester Intelligence Center
85 Court Street
White Plains, New York 10601

Agency: Chief Joe Decarlo
Greenburgh Police Department
188 Tarrytown Rd
White Plains, NY 10607

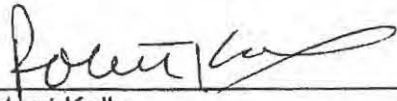
12. Compliance with Law:

WIC and Agency will comply with all applicable federal, state and local laws, codes, ordinances, rules, and regulations in performing activities under this agreement.

13. Execution of Memorandum of Agreement:

By executing this agreement, WCDAO and Agency acknowledge that they have received a copy of this agreement and will comply with its terms and conditions. This Memorandum of Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together constitute one and the same instrument. A complete original will be kept on file with WIC.

Agreed to on behalf of WCDAO and WIC:

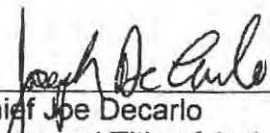


Robert Kelly,
Administrator, WIC

2/29/2012

Date

Agreed to on behalf of: Greenburgh Police Department
Law Enforcement Agency



Chief Joe Decarlo
Name and Title of Authorized Representative

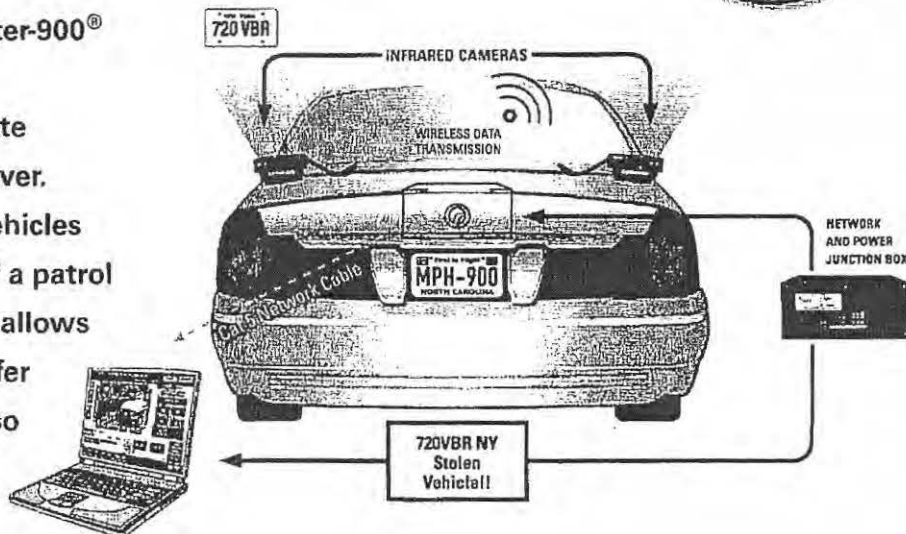
2/29/12

Date

MPH-900® AUTOMATIC LICENSE PLATE READER



The Mobile Plate Hunter-900® is the most accurate Automatic License Plate Reader technology—ever. It identifies suspect vehicles within milliseconds of a patrol car passing them and allows officers to interdict safer than ever before. It also gathers criminal intelligence data that can aid investigations.



- Captures up to 1,800 reads per minute, day or night
- Processes parked and moving vehicles across 4 lanes of traffic
- Captures plates at up to 150 mph (241 kph) closing speeds and passing speeds
- Recognizes plates from all 50 states, Canada, and Mexico and reads Arabic characters
- Finds suspect vehicles within milliseconds of passing them
- Alerts officers immediately if a vehicle is suspect, indicating the nature of the offense
- Identifies suspended and revoked drivers before they cause a crash
- Captures criminal intelligence data including date and time stamps, GPS coordinates and photo of the license plate
- Criminal intelligence capabilities aid in: *Witness identification, Watch list development, Placing suspect at a scene, Terrorist interdiction, Pattern recognition*
- Enhances effectiveness of Amber Alerts
- Secures sensitive areas with Geofencing
- Increases revenues by collecting delinquent taxes, fees, and fines
- Utilizes digital cameras available which capture much larger license plate image revealing part of the car, and its immediate surroundings

ELSAG North America, LLC, a Finmeccanica company | Global Leaders In Public Safety Technology

1 (877) 77.ELSAG | 1 (877) 773.5724 | info@elsag.com | www.elsag.com

YOUR MISSION...IS OUR MISSION.

Made In The USA

US 09/14/11



ELSAG
North America
A Finmeccanica Company

**THE MPH-900® READS PLATES FROM
ALL 50 STATES, DAY OR NIGHT**



**The power of the
MPH-900® ensures safer
streets, a safer nation,
and safer officers.
More than eleven hundred
agencies across all fifty
U.S. states are applying
the MPH-900® to a variety
of missions including:**

- Recovery of stolen vehicles
- Assistance with AMBER Alerts and missions related to missing and exploited children
- Safe school initiatives such as perimeter security and school bus safety
- Development and maintenance of Sexual Predators Hot Lists
- Drug interdiction
- Highway safety
- Homeland Security initiatives
- Gang and racketeering interdiction
- Collection of delinquent taxes, fines, and fees

The MPH-900® is the most advanced Automatic License Plate Reader available. With superior algorithm technology, no other system comes close to its ease of deployment, capabilities, and accuracy.

ELSAG North America, LLC, a Finmeccanica company *Global Leaders In Public Safety Technology*

1 (877) 77.ELSAG | 1 (877) 773.5724 | info@elsag.com www.elsag.com

YOUR MISSION...IS OUR MISSION.



Made In The USA

US 09/14/11



ELSAG
NorthAmerica
A Finmeccanica Company



2012 PRODUCT CATALOG

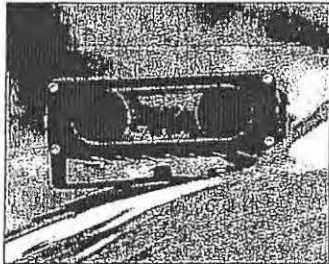
1 (877) 77ELSAG 1 (877) 773.5724



ELSAGNorthAmerica
A Finmeccanica Company

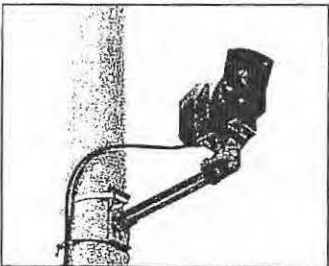
ELSAG North America, LLC. A Finmeccanica Company

 Made In The USA



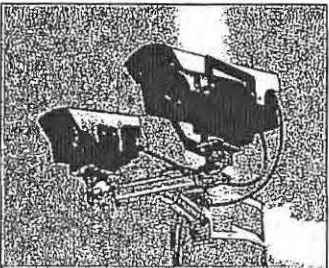
MOBILE MPH-900® ALPR SYSTEM

The MPH-900® is the most accurate mobile ALPR system available. Digital cameras mounted to the exterior of the patrol car read up to 1,800 plates per minute from a stationary location or at highway speeds, cross referencing them against a hotlist housed on the in-car computer, alarming if there is a match. Data collected can be transferred to a storage server for future analysis to aid investigations.



FIXED FPH-900® ALPR SYSTEM AND FCU-900® UTILITY BOX

The FPH-900® is a compact, digital system integrating all ALPR components inside a heavy-duty FCU-900® Utility Box. The system reads up to 1,800 license plates per minute day or night, in any weather capturing a color image of the car, GPS coordinates, and date and time stamps. When suspect vehicles are identified, alarms are broadcast wirelessly to a command center, nearby patrol vehicles and/or officers' PDAs. The FCU-900® Utility Box houses the ruggedized PC which hosts communications, along with surge and power management devices, as well as a high tolerance heater and fan for self-regulating temperature.



THE ALL-IN-ONE FIXED ALPR SYSTEM

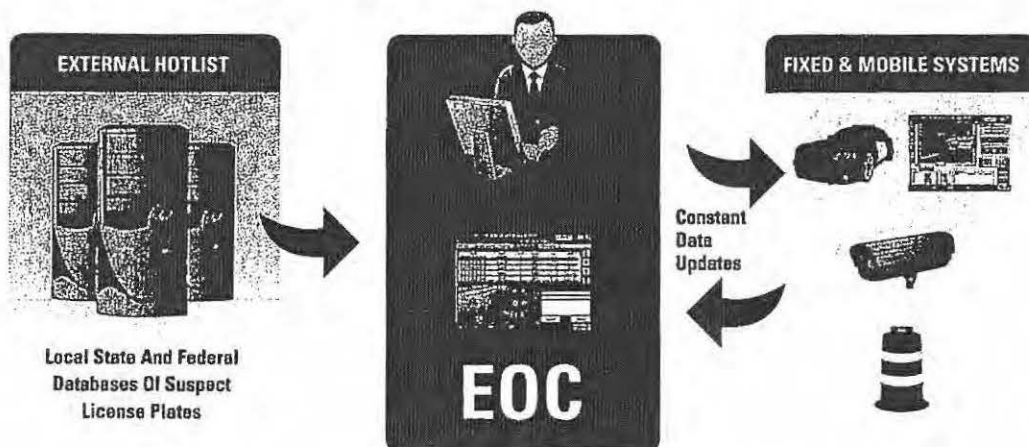
ELSAG's FPH-900® ALPR technology is now available as an All-In-One (AIO) system that combines the power of our fixed digital cameras with a hyper ruggedized mini computer. This compact, efficient system features low power consumption and can be set up anywhere, even deployed as a best of class covert solution. It features three Ethernet ports for additional FPH-900® cameras in order to support multi lane coverage and optional communication slots which support both cellular or Wi-Fi connectivity, allowing for seamless integration with ELSAG Operation Center™ software.



RADAR TRAILER

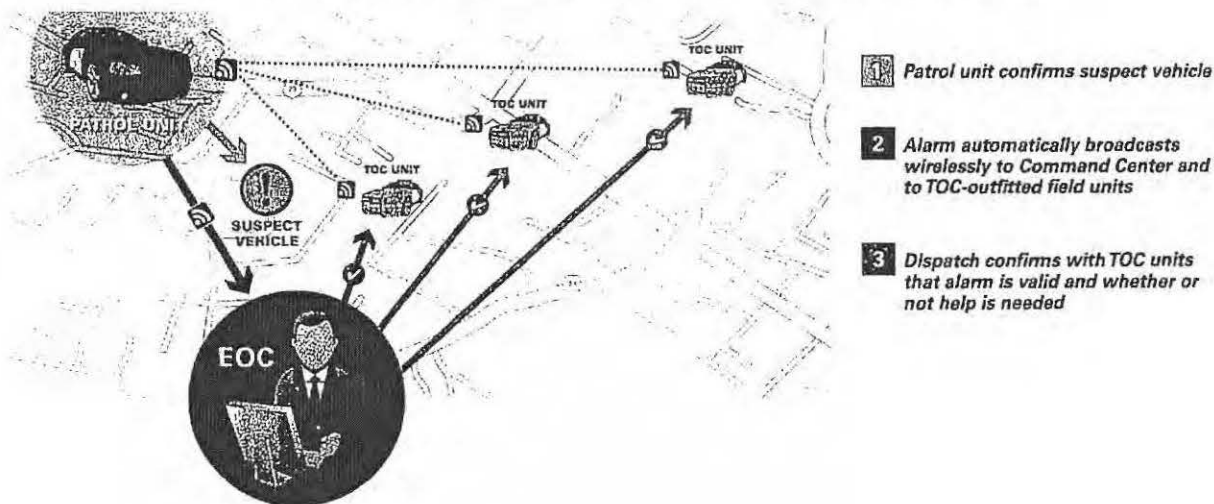
Get the benefits of speed monitoring and ALPR in one mobile solution. The DRT-1000 transforms a standard radar trailer into a powerful covert tool that identifies license plates connected to auto theft, child predators, warrants, scofflaws, uninsured vehicles, revoked driving privileges, parolees, etc. while serving as a deterrent to speeding. With the optional Emergency Power Source, 4000 watts of stored solar power are available for use during emergencies such as hurricanes, earthquakes, floods, and power blackouts.

ELSAG OPERATIONS CENTER™



Your agency's ALPR units collect vast amounts of data that help resolve issues in real time, as well as provide critical intelligence to aid investigations. The ELSAG Operations Center™ is the brain that collects, analyzes, and manages all of those intelligence assets. The EOC™ runs automatically, without user invention, communicating with all MPH-900® vehicles, cameras, and tactical operations desks in your domain, ensuring that each ALPR system is current with up-to-date information. The EOC™ saves time, resources and keeps your information safely stored.

ELSAG TACTICAL OPERATIONS CENTER™



ELSAG Tactical Operations Center™ software shortens response times and increases officer safety by broadcasting MPH-900® alarms to Dispatch and fellow officers automatically and simultaneously. This saves time during the critical period from when an MPH-900® officer receives an alarm to when backup units respond. TOC-outfitted vehicles do not have to have the MPH-900® installed in order to receive alarm information. Their TOC software works behind the scenes without officer involvement, coming to the forefront of the in-car computer once an alarm is received. As Dispatch is verifying the validity of the alarm, TOC-outfitted vehicles are already on their way to help.



With 70% of criminal activity in the U.S. involving a vehicle, and an estimated 40 million license privileges revoked, suspended or denied, the MPH-900® is critical to addressing many missions.

Real-time Intervention

- AMBER Alerts
- Auto theft recovery
- Highway and traffic safety
- Homeland Security
- Perimeter security
- Plate manipulation
- Probable cause generation
- Rental contract violations
- School bus safety

Intelligence Gathering

- Coordination with other MPH-900® systems
- "Late hit" analysis
- Link analysis
- Suspect surveillance
- Traffic pattern analysis

Revenue Collection

- Garage and lot access
- Parking enforcement
- Scofflaw violations
- Tax collection

MPH-900® AND FPH-900® COVERT ALPR SOLUTIONS

ELSAG's ALPR systems easily adapt to covert applications by concealing system components in apparatus or compartments that fit in naturally with their surroundings. We continually work with partner agencies to develop creative covert solutions that address their specific needs, many of which are becoming best practices across the country for missions requiring undercover surveillance or inconspicuous "private eyes" along roadways and in other areas. All fixed and mobile covert products are crafted individually in our manufacturing facility in Greensboro, NC. Each one undergoes a battery of tests and must pass strict quality standards before being delivered and installed.

THE MPH-900® IN ACTION



Digital Automatic License Plate Recognition cameras are attached magnetically to the body of the patrol car.

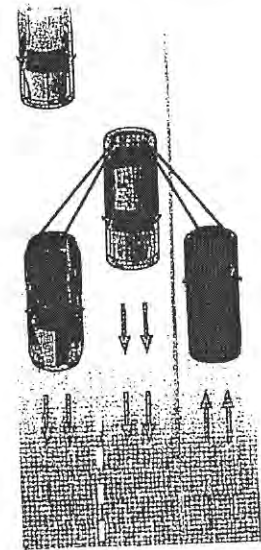
- 1** Officers on roadways use cameras to scan plates of passing cars.
 - Cameras can read plates from fast-moving vehicles.
 - Locations and times of captured plates are stored.
- 2** An infrared camera captures images of the plate.
- 3** A computer reads the plate characters and compares them with crime databases.

JAN California
000-01T8

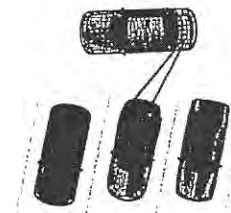
000-01T8

Officers are alerted of a match.

Database
Y01-N010
000-01T8
P93-F6L4
400-591T



Cameras can also scan in parking lots.



The MPH-900® Performance

- Captures up to 1,800 reads per minute, day or night
- Processes parked and moving vehicles across 4 lanes of traffic
- Captures plates at up to 150 mph (241 kph) closing speeds and passing speeds
- Recognizes plates from all 50 states, Canada, and Mexico
- Finds suspect vehicles within milliseconds of passing them
- Alerts officers immediately if a vehicle is suspect, indicating the nature of the offense
- Captures criminal intelligence data including date and time stamps, GPS coordinates and photo of the license plate
- Enhances effectiveness of Amber Alerts
- Secures sensitive areas with Geofencing