Pennsylvania State Police

COMMONWEALTH LAW ENFORCEMENT ASSISTANCE NETWORK

ADMINISTRATIVE REGULATIONS

Version 4.7

Bureau of Communications and Information Services

1800 Elmerton Avenue

Harrisburg, PA 17110

Telephone: 717-783-5575

Fax: 717-772-1434

Website: www.psp.state.pa.us

Revisions

Date	Version	Description	Author
1/12/2009	V0.1	Created	Deb Pipes
2/6/2009	V0.2	Formatted and language changes	Shawn Sanders
2/9/2009	V0.3	Added Merv & Wendy changes	Shawn Sanders
3/2/2009	V0.4	Added Debs (definitions)	Shawn Sanders
9/14/2009	V0.4.1	Edits and formatting	M. Rodriguez
9/15/2009	V0.4.2	Added acronym section and expanded section 14.1 Dissemination of CHRI	M. Rodriguez
1/20/10	V0.4.3	Edits and formatting	J. Winkowski
03/26/10	V0.4.4	Edits and formatting	J. Winkowski
07/08/10	V0.4.5	Edits and formatting	J. Winkowski
10/28/10	V0.4.6	Language changes. edits & formatting	Pedro A. Rivera
01/07/10	V0.4.7	Edits and Formatting	J. Winkowski

Table of Contents

FOREWORD

The Commonwealth Law Enforcement Assistance Network (CLEAN) is administered by the Pennsylvania State Police (PSP).

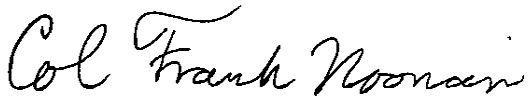
The PSP Commissioner, as outlined in Title 71 Pa.C.S. 250 (f) and 251 (a), is responsible for establishing policy procedure and regulations consistent with state and federal law, regulations, and policies by which CLEAN is administered.

The PSP is contractually designated by the Federal Bureau of Investigation (FBI) to serve as the Criminal Justice Information Services (CJIS) System Agency (CSA) and, as such, serves as the sole point-of-contact for CJIS and the International Justice and Public Safety Information Sharing Network (Nlets). The PSP also appoints a CJIS Systems Officer (CSO) and Information Security Officer (ISO) to handle all CJIS and Nlets criminal justice matters, as well as liaison activities with the other 49 states and U.S. territories. Currently, CLEAN has over 20,000 certified users and supports information requests from many different criminal justice agencies including over 23,000 Pennsylvania dedicated sworn law enforcement officers. As such, CLEAN serves as the foundation for criminal justice information sharing within Pennsylvania and among the Commonwealth's federal, state, and local partners. CLEAN continues to be the quickest, most reliable and trusted broker of criminal justice data in the Commonwealth.

The purpose of the CLEAN Administrative Regulations Manual is to provide an available reference to the policies and procedures of the CLEAN and CJIS systems.

The regulations contained in this manual consist of provisions necessary for the efficient and effective operation of the CLEAN and CJIS systems.

The provisions and various sections and paragraphs of these Administrative Regulations are severable. If any provision(s), section(s), or paragraph(s) contained herein is contested or held to be unconstitutional, the decision so holding shall not be construed as affecting or impairing any other provision, section, or paragraph of these regulations as a whole.



Colonel Frank Noonan
Acting Commissioner

A) PURPOSE

1) The CLEAN system is a statewide computerized information system established in September of 1971. The CLEAN system is a 24 hour a day, 7 days a week operation which provides the criminal justice/law enforcement communities with validated criminal justice information. As stated in the Foreword, the PSP through the CSO is the sole point-of-contact with CJIS and the Nlets systems. In order to ensure that the CLEAN system is managed effectively and efficiently, and that the usage of the CLEAN system is appropriate, the PSP has developed the "Core Purpose" for the CLEAN system.

B) CLEAN CORE PURPOSE

1) In the furtherance of officer safety and the administration of justice; ensure the secure delivery of timely, accurate and relevant criminal justice information to authorized agencies.

C) CLEAN ADMINISTRATIVE SECTION

1) The operational guidelines, procedures and policies, as well as system access, training, validations, audits, operator certification, quality control, integrity, and security are controlled by the PSP, CLEAN Administrative Section, in particular, the State CJIS (CSO). The CSO reports to the Director, Bureau of Communications and Information Services, through the Director, Dispatch Operations Division.

2) An opinion with regard to interpreting any portion of the CLEAN Administrative Regulations may only be given by the CSO or designated alternate within the CLEAN Administrative Section.

D) FUNCTION OF CLEAN

1) The CLEAN system maintains accessible files on Stolen Vehicles, Stolen Vehicle Parts, Stolen License Plates, Wanted/Missing Persons, and Protection from Abuse Orders. These same records are also forwarded to and accessible at NCIC. Other "Hot File" records are forwarded to NCIC.

2) The CLEAN system is not the Central Repository for Computerized Criminal History Record Information "CCHRI."

E) THE CLEAN SYSTEM INTERFACES WITH THE FOLLOWING AGENCIES:

1) **National Crime Information Center (NCIC)**-

NCIC 2000 is a nationwide, computerized information system established as a service to all criminal justice agencies--local, state, and federal to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information. For NCIC 2000 purposes, criminal justice information is defined as "information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function."

2) **International Justice and Public Safety Information Sharing Network (Nlets)-**

Nlets provides two basic capabilities to its users. First, it is an international, computer-based message switching system that links together state, local, and federal law enforcement and criminal justice agencies for the purpose of information exchange. Second, it provides information services support for a growing number of criminal justice related applications. To accomplish this, Nlets supports data communications links to state networks using a commercial frame relay service. All agencies within each state are serviced through this state interface. Federal and international systems operate in much the same manner. The primary Nlets operational site is located in Phoenix, Arizona, with a disaster recovery site located with the Idaho State Police that is capable of providing full continuity of operations in less than thirty minutes.

3) **Pennsylvania Department of Transportation, Bureau of Motor Vehicles (BMV)-**

Pennsylvania Department of Transportation (PennDOT) provides vehicle registration, operator license numbers, drivers' histories, title numbers, and drivers' license photographs via JNET.

4) **Pennsylvania Fish and Boat Commission**-

Protects, conserves, and enhances the Commonwealth's aquatic resources and provide fishing and boating opportunities. They provide automated Boat registrations to CLEAN/NCIC users.

5) **Pennsylvania Central Repository-**

The Pennsylvania Central Repository is the central location for the collection, compilation, maintenance, and dissemination of Criminal History Record Information (CHRI) by the PSP. The repository was created and is maintained in accordance with Pennsylvania's Criminal History Information Act (CHRIA) contained in Chapter 91 of Title 18, Crimes Code. This Act also directs The PSP to disseminate criminal history data to criminal justice agencies, non-criminal justice agencies and individuals on request. Criminal Justice/Law Enforcement agencies can access all of an individual's criminal history record information (CHRI). Requests made by non-criminal justice agencies and individuals are subject to edit criteria contained in the law. The Central Repository is the responsibility of the Bureau of Records and Identification within the PSP.

6) **Commonwealth Justice Network (JNET)-**

a) JNET is the Commonwealth's public safety and criminal justice information broker. JNET's integrated justice portal provides a common on-line environment for authorized users to access public safety and criminal justice information. This critical information comes from various contributing municipal, county, state, and federal agencies.

7) **Philadelphia Police Department System (PCIC)-**

a) The Philadelphia Police Department maintains their own NCIC circuit and Systems.

F) THE CLEAN USERS ARE PROVIDED WITH THE ABILITY TO:

1) Transmit and receive law enforcement related messages from other devices connected to CLEAN.

2) Communicate with other states and Canada through Nlets.

3) Enter or retrieve information from CLEAN Stolen Vehicle, License Plate, Wanted and Missing Person, and PFA files.

4) Enter into and retrieve information from National Crime Information Center (NCIC)"Hot Files".

5) Access criminal history data from the Interstate Identification Index (III).

6) Access criminal history data from the Pennsylvania Central Repository.

7) Obtain information from the PennDOT on vehicle ownership, driver's licenses, and to generate on-line requests for driving history records.

8) Obtain registration information on all Pennsylvania registered boats from the Pennsylvania Fish and Boat Commission.

9) Access to Nlets files (e.g. Parole, Probation and Corrections, Hazmat files).

10) Access to NCIC files (e.g. ORI, VGTOF, and Foreign Fugitive).

G) OFFICIAL USE OF CLEAN INFORMATION

1) The CLEAN system is for appropriate criminal justice and law enforcement purposes only. All traffic generated over the system shall be made in the performance of the employee's or agencies official duties as they relate to the administration of criminal justice or authorized by law. At no time shall an inappropriate message or non-criminal justice information be allowed to be generated over the CLEAN system. The transmission of an inappropriate message or non-criminal justice information over the CLEAN system is a violation of this policy. The dissemination of operator, vehicle, vehicle owner, social security or criminal history information obtained from or through CLEAN to anyone outside the criminal justice or law enforcement community is strictly prohibited. Prohibited acts include, but are not limited to:

   a) Unauthorized dissemination (e.g. giving friends or family any information received from CLEAN).

   b) Unauthorized access (e.g.. running transactions through CLEAN to locate friends/family or for other personal reasons).

   c) Criminal conduct; using the information accessed from CLEAN to perpetrate a crime (e.g. harass or stalk someone).

2) All users must adhere to all CLEAN administrative regulations and appendices.

H) SYSTEM REQUIREMENTS FOR ACCESS to CLEAN SERVICES

1) Requests for assignment or modification of ORI numbers must be made in writing to the CJIS (CSO). These requests are to be addressed to the Commander, CLEAN Administrative Section; Pennsylvania State Police Headquarters 1800 Elmerton Ave, Harrisburg Pa. 17110. Upon receipt, the requests will be evaluated by the CSO staff to determine if the agency meets the criteria for ORI assignment. Once a determination has been made, the requesting agency is notified of the decision in writing.

2) Correspondence requesting the issuance of an ORI must include:

   a) Type of ORI requested.
   b) Agencies goals and objectives.
   c) Agency organizational table.
   d) A copy of the Resolution, State Statute (including court response, if required) creating your agency and/or giving your agency criminal justice authority.
   e) Scope of authority (i.e. investigative authority, statutory authority etc.).
   f) Training documentation as required by House Bill No. 564, Session of 2003. Please note that House Bill 564, of 2003 now requires all employees (including police officers) of a public school system to have a criminal background check completed.

3) Depending the type of ORI requested, the following would also need to be included in the correspondence:
   a) Court Order
   b) Oath of Office
   c) Act 120 training certificate
   d) Criminal Background check.

4) A valid ORI is mandatory for access to the CLEAN/CJIS system.

5) Any agency in Pennsylvania desiring an ORI shall make a written request to the CLEAN Administrative Section. Accompanying the written request shall be a copy of the statute or ordinance that establishes such agency and describes the agency's functions and authority. The CSO shall, if applicable, assign an ORI. If the request is denied, the CSO shall provide written findings to the agency that requested the ORI outlining the reason for denial.

6) The ORI determines the extent of access to CLEAN, NCIC, or Nlets as follows:

   a) **Full Access ORI's** – Are authorized access to all NCIC 2000 files and the Interstate Identification Index (III). Full access ORI's are assigned to Criminal Justice/Law Enforcement agencies having law enforcement authority for the administration of criminal justice. The data transmitted by the CLEAN and the NCIC systems is documented criminal justice information and access to that information is restricted to duly authorized agencies. Such agencies are those meeting the definition of a Criminal Justice Agency in Title 18 Pennsylvania Consolidated Statutes, Chapter 91 (9102) and the United States Department of Justice definition of a Criminal Justice Agency, as contained in the Code of Federal Regulations (Title 28-Judicial Administration, Part 20). Additional agencies that qualify for the full Access ORI are: (1) County Children and Youth are issued full access ORI's ending in a F, (2) Courts that hear Domestic Violence and stalking cases, (3) Non Governmental railroad or Campus Police Departments.

b) **Limited Access ORI's** - Are authorized access to a limited number of NCIC files. Nongovernmental agency or subunit thereof, which allocates a substantial part of its annual budget to the administration of criminal justice, and whose regularly employed peace officers have full police powers pursuant to state law and have complied with the minimum employment standards of governmentally employed police officers as specified by state statute, may have direct terminal access to NCIC 2000 U.S. Secret Service Protective, Wanted Person, Missing Person, stolen property files, and active Protection Order File records, provided such access is approved by the CSO. Public Housing Authority's have III (QH) access only.

c) **Limited Department of Motor Vehicles (DMV) Access ORI's** – Limited access ORI's for Driver and Vehicle information is available from some states. This ORI ends in VS. In Pennsylvania Parking Authorities and Code Enforcement Offices can have access to Pennsylvania Hot Files, PennDOT vehicle registration files, PennDOT operator license files and PA Instate only BMV.

d) **State Assigned Judiciary ORI** - This ORI is to accommodate the agency's needs for issuing citations and the appropriations of monies collected as a result of an enforceable violation. This state ORI is assigned to identify your agency within the Commonwealth of Pennsylvania to the Administrative Office of Pennsylvania Courts (AOPC). If your agency is granted this ORI, there is no access to the CLEAN or NCIC files.

Note: Refer to Appendix D for the proper procedures for obtaining an ORI.

I) EQUIPMENT, MAINTENANCE, AND SUPPORT REQUIREMENT

1) As a condition of maintaining access to CLEAN, all agencies currently using CLEAN shall acquire their own equipment; including, but not limited to, personal computers, software, and printers for operation as specified by the PSP. Authorized agencies shall also be responsible for:

2) All types of maintenance associated with CLEAN Secure User Station, including all equipment and communication lines.

a) Acquiring all necessary supplies associated with CLEAN Secure User stations.

b) All costs associated with the installation or relocation of equipment and data communication lines, and:

c) Paying annual recurring costs to the Commonwealth associated with data communication lines.

3) Security Enforcement:

a) Conformance to CLEAN security standards.

b) Any agency accessing CLEAN Services shall be responsible for enforcing system security standards as defined by the CLEAN Information Security Policy, the CJIS Security Policy and this regulation. Security standards instituted by any agency accessing CLEAN services shall, at a minimum conform to the CLEAN Administrative Regulation, the CLEAN Information Security Policy and CJIS Security Policy. Agencies may enact stricter standards; however, the standards shall not be less restrictive.

c) All devices connected to or having access to the CLEAN system shall be agency owned and managed.

4) Any agency accessing CLEAN services shall have documented procedures in place to monitor all security policies and have a written policy for the discipline of violations of the CLEAN Administrative Regulations, the CLEAN Information Security Policy, CJIS Security Policy and Nlets Security Policy.

a) Appointment of Local Agency Information Security Officer (LAISO): Agencies accessing CLEAN services shall appoint a LAISO as the security point of contact and liaison between CLEAN and the local agency.

Reference Appendix C: Information Security Procedures for LAISO responsibilities.

J) SECURITY AWARENESS AND TRAINING

1) Requirement:

a) Agencies shall ensure that all personnel who access CLEAN and FBI CJIS systems attend security awareness training at least once every two years.

b) All new employees and all appropriate IT personnel who have access to CLEAN and FBI CJIS systems shall have attended security awareness training prior to access.

c) Documentation: Agencies shall document which employees have received security awareness training along with the materials used to present the training. This documentation shall be available for review during an audit of the agency.

K) PERSONNEL REQUIREMENTS

1) This section **does not** apply to individuals whose CLEAN access has been suspended, revoked/terminated by the CLEAN Administrative Section. This section does pertain to any person who receives information from the CLEAN system.

2) A CLEAN system operator is a person 18 years of age or older, who has been certified and/or trained through the CLEAN Administration Section.

3) Application Procedures for New Users

   a) National fingerprint-based record check: The agency applying for CLEAN access shall cause a national finger-print based background check to be conducted on all individuals who will have any access to the CLEAN system. "Access" shall be defined as, "Opportunity to make use of an automated information system resource which transmits, receives, stores or processes CLEAN or CJIS data; the ability to have contact with a CLEAN workstation from which a transaction may be initiated." The term "access" does not include individuals who, as part of their official duties, review case files containing hard copies of information received through CLEAN.

   Note: Reference Appendix E: Operators Certification Manual.

   b) Agency Employees: Employees having access to CLEAN workstations and systems shall have a fingerprint-based background check completed prior to the individual being allowed access. This includes those individuals who have direct responsibility to configure and maintain computer systems and networks with direct access to CLEAN systems. Such background checks shall include a state and national fingerprint-based search for a criminal record. Should a criminal record exist, the hiring agency shall review the record in its entirety and determine whether the individual is disqualified from accessing CLEAN.

   c) Vendors and Contractors: Support personnel, contractors, custodial workers and individuals who have direct responsibility to configure and maintain computer systems and networks with direct access to CLEAN workstations and systems, shall have a fingerprint-based background check completed prior to being allowed access, unless these individuals are escorted by authorized personnel at all times. Such background checks shall include a state and national fingerprint-based search for a criminal record. Should a criminal record exist, the authorized agency (e.g., police department, 911 Center) shall review the record in its entirety and determine whether the individual is disqualified from accessing CLEAN system.

Note: "Authorized personnel" are those persons who have passed a state and national fingerprint-based record check and have been granted CLEAN access.

L) CLEAN ACCESS DISQUALIFIERS

1) Prohibited Individuals:

   a) Individuals **shall not** have access to CLEAN systems nor be eligible to become certified as a CLEAN System Operator if it is found in their criminal history that any of the following has occurred:

   b) a conviction, or is under indictment for any felony.

   c) a conviction, or is under indictment for any misdemeanor for which more than 1 year in prison can be imposed as punishment, except in ARD applicable cases.

   d) a conviction, or is under indictment for any computer crime.

   e) Computer Crimes, as used in this section refer to Pa Title 18 Crimes and Offenses Chapter 76 Computer Offenses or the equivalent penalties as provided by the laws of any other state, territory, or under federal law.

      Note: The CSO or his designee can deny an individual access to the CLEAN system for just cause.

2) Ten Year Rule: Individuals shall not have access to CLEAN systems nor be eligible to become certified as a CLEAN System Operator for 10 years from the date of disposition for any of the following convictions found in their criminal history

   a) Any misdemeanor for which the individual was incarcerated for 30 days or more.

   b) any two misdemeanors which occurred in separate incidents, within the last 10 years except in ARD applicable cases.

3) Grading: Misdemeanor 1, 2 and 3, and felony as used in this section refers to any misdemeanor 1, 2 and 3, and felony under the laws of Pennsylvania, or the equivalent penalties as provided by the statutes of any other state, territory, or federal law

4) Temporary Suspension: If an individual, who has access to CLEAN information, is arrested or indicted for **any** of the following, that individual will lose access to CLEAN information until the charges are disposed of in court-

   a) Felony

   b) Misdemeanor for which more than one year in prison can be imposed as punishment, except in ARD applicable cases.

   c) Computer crime.

   d) Misdemeanors where there are two or more counts from separate criminal complaints/incidents, except in ARD applicable cases.

5) Revocation: An individual will have their CLEAN access revoked for life for a conviction of **any** of the following-

   a) Felony

   b) Misdemeanor for which more than one year in prison can be imposed as punishment except in applicable ARD cases

   c) Computer crime.

6) Suspension:

   a) An individual will be suspended from CLEAN access for **10 years** if convicted and incarcerated for any misdemeanor 2 except in applicable ARD cases.

   b) An individual will be suspended from CLEAN access for **1 year** if convicted and incarcerated for more than 72 consecutive hours for any misdemeanors

M) PHYSICAL SECURITY

1) Computer Facility Security:

   a) The computer site and related infrastructures (e.g., information system servers, controlled interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc., including police vehicles if they house equipment which provides access to the CLEAN network) must have adequate physical security at all times to protect against any unauthorized access to, or routine viewing of, computer devices, access devices, and printed and stored data.

b) Law enforcement sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

c) All visitors to computer facilities with access to CLEAN systems or workstations shall be escorted by authorized personnel at all times.

d) All changes concerning the equipment connected to CLEAN/NCIC must be coordinated through the CLEAN Administrative Section including relocation of equipment, upgrading existing equipment, and acquiring additional equipment. All equipment and manuals must be placed in an area that is secure from access by unauthorized persons.

e) Scheduled downtime requires notification by the agency TAC/Alternate TAC to the CLEAN Administrative Section. Do not disconnect, turn off, alter any connections or access to or from, or add any peripherals to your CLEAN/NCIC equipment without notifying the CLEAN Administrative Section as this could affect the response time for other agencies.

2) CLEAN Equipment:

a) The CLEAN system equipment must be safeguarded from damage by excessive dirt, employee misuse, fire, floods, and power failure.

b) If any damage occurs, it will be reported to the CLEAN Administrative Section by telephone or by switch message. Agencies will be liable for payment for repairs to the CLEAN router or if applicable other supplied equipment resulting from negligence, abuse, or misuse.

c) Failure to maintain a secure site will be a violation of this policy.

d) CLEAN circuit equipment must be located in an area which follows manufacturer guidelines and allows it to operator properly.

Note: Agencies behind interfaces should contact the Interface Agency computer personnel prior to contacting the computer center (i.e., personnel with JNET access should contact their JNET TAC). PSP personnel who intend on using JNET applications are referred to Appendix F PSP Use of JNET for guidance.

3) Media Security: When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process CLEAN data shall be destroyed by shredding (which must occur before destruction), incineration, or degaussing, considering whichever method is available, appropriate, and cost effective. This list is not all-inclusive. IT systems which have processed or stored CHRI shall not be released from control until the equipment is sanitized and all stored information has been cleared.

4) Media Reuse: IT storage media that will be reused by another entity shall be sanitized. The steps taken to sanitize shall be documented by the releasing agency.

Note**:** Reference Appendix C: Information Security Procedures.

N) STANDARD AGREEMENTS

1) Criminal Justice Agency Agreement:

a) As per the CJIS security policy, criminal justice agencies requesting CLEAN access shall sign a CLEAN agreement certifying that the agency administrator has read and understands the requirements as a condition of access to CLEAN. The terms of the agreement are not optional and may not be modified. This agreement will specify the CLEAN services the agency will have access to and reference the CLEAN and FBI CJIS policies which the agency must adhere to.

b) Agreements shall be updated at least once every audit cycle.

c) Agreements shall be updated when a change is made to the chief executive officer of the agency.

d) The agreement between the direct connect agency and the interface agency shall incorporate the CLEAN administrative regulations, FBI CJIS Security Policy and FBI CJIS security addendum in addition to any requirements set by the direct connect agency. A copy of all such agreements shall be retained for inspection. Review of agreements shall be conducted by the CLEAN audit/investigation unit.

e) The CLEAN Administrative Section shall be notified by the interface agency of any change of services to connected agencies.

f) Any contract changes in your agency which would affect the operation or management control of the CLEAN/NCIC system (such as privatization) must be brought to the attention of the CLEAN Administrative Section prior to such changes.

g) Secondary Connections: A Criminal Justice Agency (CJA) with direct access to CLEAN (Direct Agency) services may permit another authorized agency to access CLEAN services through their established connection. Prior to permitting such a connection the CJA shall enter into an agreement with the connecting Interface Agency.

2) Servicing Agency Agreement:

a) Any authorized agency with direct or indirect access to CLEAN must enter into a direct or indirect agreement. The agreements will be provided either in hard or electronic copy by the CLEAN Administrative Section.

b) The direct access agency will enter into an agreement with the CLEAN Administrative Section. The direct access agency will update the agreement every audit cycle or if any of the agreement signatures leave the agency. The original will be forwarded to the CLEAN Administrative Section.

c) The indirect access agency will enter into an agreement with thet agency that has direct access to CLEAN. The agreement that shall be used is provided by the CLEAN Administrative Section. The servicing agreement must be signed by the direct (servicing) agency and the indirect agency. The servicing agency will retain the original. These agreements are subject to review during a CLEAN audit. Copies will **not** be forwarded to the CLEAN Administrative Section. Any agency responsible for the management control of the direct (servicing) agency shall enforce the CLEAN administrative regulations with the indirect agency.

d) A non-criminal justice agency may gain access to CLEAN/Nlets, but not CJIS, pursuant to a specific agreement with a direct agency and only upon approval of the CLEAN Administrative Section.

e) Any variances from standard terms made in servicing agreements must be cleared through the CLEAN Administrative Section before being signed.

3) Management Control Requirements: An agency (e.g., Communication Centers, 911 Centers) not meeting the qualifications or definition of a CJA must be under the management control of a CJA. The degree of management control shall be such that the agency having management control has the authority over that portion of the computer electronic switches, satellite computers and workstations, and other devices interfacing directly with the CLEAN system.

4) Memex Agreement: MEMEX is an automated intelligence/investigative system network that exist separate and apart from CLEAN. However, as CLEAN, NCIC, and Nlets can be accessed through MEMEX on authorization, rules for each come into play. CLEAN policy and regulations must, therefore, be observed in appropriate situations. Access to CLEAN through MEMEX terminals will not be provided until an agreement is reached and signed.

5) LiveScan/IAFIS Agreement: As a condition to connectivity and/or access to the CLEAN system to transfer data, eligible agencies shall enter into a written agreement between the CJIS Systems Agency (CSA) and the authorized agency. The agreement will include all mandates i.e. training, security, proper use, standards, etc., as required per the current CJIS Security Policy and this policy

   Note: Reference all appendixes for specific requirements that direct and indirect agency's must follow.

O) TERMINAL AGENCY COORDINATOR (TAC)

1) Every agency directly connected to CLEAN must have personnel designated as the TAC and Alternate TAC. Each agency administrator shall designate individuals who have been certified CLEAN operators for at least one year and attended an approved CLEAN training unit program. All TAC officers must be approved by the CLEAN Administrative Section. They must attend all mandatory training as directed by the CLEAN Administrative Section.

2) The TAC and Alternate TAC are individuals assigned by and employed by their respective agency to act as a liaison between the user agency and the CJIS system agency PSP. All requests concerning CLEAN and CJIS must be coordinated through the user agency TAC or Alternate TAC.

3) Troop Communication Specialist (TCS): Among their duties, a TCS assumes all the applicable duties of a TAC/Alternate TAC as referenced in Appendix H and OM 7-8, Chapter 2.

P) OPERATOR CERTIFICATION

1) Operator Certification is a state and federally mandated program which requires knowledge and proficiency testing concerning the CLEAN/CJIS network. New operators shall be appropriately certified in their authorized access level within six months of assignment as a CLEAN operator. There are four levels of access for the CLEAN system,

   Note: Reference Appendix E: Operator Certification

Q) VALIDATIONS

1) The agency TAC/Alternate TAC ensures that the validation officer completes the monthly validations in a timely manner and documents the validation results in conformance with the CLEAN Administrative Sections procedures.

   Note: Reference Appendix I: Validation Manual.

R) HIT CONFIRMATION

1) Any agency that receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions based upon the hit NCIC record:

   a) Arresting the wanted person.

   b) Detaining the missing person.

   c) Seizing the stolen property.

   d) Charging the subject with violating a protection order. Additionally, an agency detaining an individual on local charges where the individual appears identical to the subject of the wanted person record *and is within the geographical area of extradition* must confirm the hit.

2) When receiving a hit confirmation request, the official record holder must respond within 10 minutes for urgent requests, or one hour for routine request, with the desired information. A notice of a specific amount of time necessary to confirm or reject the record may be given.

3) When an agency receives a 3rd hit request the CLEAN Administrative Section will send a letter to the agency asking for an investigation as to why this happened.

   Note: Reference Appendix B: Hit Confirmation Manual

S) CRIMINAL HISTORY RECORD INFORMATION (CHRI)

1) Dissemination

   a) CHRI accessed through CLEAN is available for dissemination by authorized personnel to criminal justice agencies for criminal justice purposes:

(1) To Federal Agencies authorized to receive it pursuant to Federal Statute or Executive Order.

(2) For issuance of press releases and publicity designed to affect the apprehension of wanted persons in connection with serious or significant offenses.

(3) Civil and criminal courts for use in domestic violence and stalking cases pursuant to Title IV, Subtitle F, of the Violent Crime Control and Law Enforcement Act of 1994, amended 28 USC 534 (e):

(4) Children and Youth Services.

b) A facsimile machine may be used to transmit III/CHRI information provided that:

(1) Both agencies involved have an ORI authorized to receive criminal history information.

(2) The machines (receiving and transmitting) are monitored during the transmission.

(3) The receiving agency shall be contacted to ensure the information was received and retrieved.

(4) Secondary dissemination is recorded (applies when III is being faxed to another agency).

2) Dissemination to Non-Criminal Justice Agencies:

a) CHRI accessed through CLEAN is available for dissemination by authorized personnel to non-criminal justice agencies authorized by law pursuant to Public Law 92-544 (86 Stat. 1115) for use in connection with licensing for local/state employment or for other uses, only if such dissemination is authorized by Federal or State Statutes.

b) Public Housing Agencies pursuant to the Housing Opportunity Program Extension Act of 1996, Public Law 104-120, for the purpose of determining whether a tenant of or an applicant for public housing may have a Criminal History Record registered on the Interstate Identification Index (III).

c) Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the dissemination of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. Social Security Number (SSN) information must also be closely guarded. At no time should the complete SSN be transmitted, only the last four digits should be used as a check.

d) Acceptable methods of destroying data obtained from CLEAN/NCIC are shredding, burning, or elimination of identifying information. Unsecured faxing and emailing of CHRI is not permitted.

3) Documentation Of Secondary Dissemination:

a) Each criminal justice agency receiving an III/CHRI response shall record any secondary dissemination of any III/CHRI to another criminal justice agency, or an individual within another criminal justice agency, or to anyone legally entitled to receive such information that is outside the original receiving agency. The III/CHRI dissemination log shall be maintained for at least 12 months. Secondary dissemination logs shall be available for audit.

b) PSP, Central Repository shall maintain an automated log of CHRI inquiries forever. The automated log will contain the following information as supplied by the operator on the inquiry screen:

(1) Date of inquiry.

(2) Name of record subject.

(3) State Identification Number (SID) or FBI number of the record subject.

(4) Purpose Code.

(5) Attention field; when querying III full name of the authorized person requesting information who is the initial user of the record. Also include a reason for the request i.e. Incident number, Case number, Citation number, or TS (traffic stop) immediately after the name. If you are using TS you must be able to articulate just cause for the query. For CLEAN/JNET users, you will find a reason field. (Requester's name on attention field cannot be the same person as the subject of the record.)

c) Agencies responding to an out-of-state request for CHRI through Nlets (Supplemental Information Request FS AQ) shall only respond with CHRI received within their agencies and maintained in their files. Out-of-state agencies requesting a statewide criminal record check shall be directed to use the PSP Central Repository.

4) Accessing of CHRI:

a) Any accessing of or inquiry into CHRI via CLEAN must be made with the proper Purpose Code and must be for the intended transaction or purpose for which the Purpose Code is designed. Purpose codes can be found in the NCIC Manual.

b) Any accessing of or inquiry into the III or Pennsylvania Central Repository using an improper Purpose Code, resulting in a record being routed to a device and displayed on the screen, shall be a violation of this policy.

c) Any dissemination by a certified operator for an unauthorized purpose, or to an unauthorized requester, shall be a violation of this policy.

d) **At no time** shall an individual be authorized to request THEIR OWN Criminal History Record Check (Requester's name on attention field cannot be the same person as the subject of the record). It shall be a violation of this policy if someone requests their own criminal history.

5) Authorized Criminal History Checks:

a) The following are authorized criminal history checks under the administration of criminal justice:

(1) Screening application for firearms and related permits (dealers, purchasers, carriers of concealed weapons, explosives dealers and users, and lethal weapons dealers and users), but only when a federal, state, or local law/ordinance exists making the criminal justice agency responsible for the issuance of the licenses/permits.

(2) Protective services pertaining to the physical protection of authorized persons (dignitaries) both foreign and domestic. This principle extends to local officials for whom protection is provided and includes record checks on personnel to be present at the site of dignitary appearances.

(3) The security of prison facilities to include, for example, record checks necessary to screen visitors, approve mail lists, and authorize vendor's access to facilities.

(4) Matters involving a violation of U.S. Immigration Laws that include both criminal actions that lead to criminal charges and administrative actions that lead to deportation.

b) **Criminal history obtained via the CLEAN system <u>cannot</u> be used for other licensing or non-criminal justice employment purposes.** For other purposes, requesters must contact the Central Repository and pay the appropriate fees if required.

Note**:** Routine record checks on personnel and random checks of visitors at non-criminal justice facilities, such as airports, shipyards, and most government buildings, are **<u>not</u>** considered to be functions within the administration of criminal justice.

6) Background Checks Only

a) CLEAN/CJIS may be used for background checks on criminal justice employees, criminal justice investigations, criminal justice administration, background checks conducted for firearms purchase, and for other lawfully authorized purposes.

b) Non-criminal justice employment background checks CANNOT be processed via CLEAN/CJIS, unless authorized by law.

c) All other request for processing of background checks for non-criminal justice employment shall be submitted in writing using the proper forms.

d) Unauthorized background checks are system integrity violations that could result in individual revocation or agency termination.

7) Individual's Right To Review: a) An individual, or his/her legal representative, may obtain a copy of his/her own Criminal History Record by submitting a written request to the PSP, Bureau of Records and Identification, 1800 Elmerton Avenue, Harrisburg, Pennsylvania 17110-9758.

8) Violations of CHRII:

a) Any investigation into misuse of CHRI from the CLEAN system which arises to criminal intent shall be referred to the Pennsylvania Office of Attorney General for a prosecutorial decision.

b) Systematic unauthorized dissemination of CHRI by an agency to an unauthorized source shall be a violation of this regulation.

T) AUDITS

1) The CLEAN Administrative Section shall triennially audit all CLEAN direct agencies. Servicing agencies shall triennially audit indirect agencies.

2) The audit shall be conducted to ensure agency compliance with CLEAN/CJIS regulations, as well as federal and state statutes on security and privacy of CHRI.

3) The CLEAN Administrative Section reserves the right at its discretion to audit any agencies receiving CLEAN/CJIS information to ensure compliance with applicable rules, regulations, security standards and this policy.

4) The CLEAN Administrative Section may conduct a mail-in audit in place of an on-site audit at selected agencies.

   Note: Reference Appendix A: Audit/Investigation Manual.

U) INVESTIGATIONS

1) The CLEAN Administrative Section shall be notified of all misuse complaints and will conduct investigations into any allegations of system misuse or misuse of information obtained through CLEAN/CJIS system.

2) The ISO shall also have the right to investigate any allegations of system integrity (i.e., security breaches).

3) There are three types of investigations:

   a) Full Investigation - Conducted by a member of the CLEAN Administrative Section reported on General Investigation Report.

   b) Limited Investigation – Conducted by a member of the CLEAN Administrative Section and reported on Department Correspondence and clearly establishes that at least one of the following applies:

      (1) The alleged misuse failed to constitute a violation of CLEAN/CJIS policies and regulations.

      (2) The complainant was mistaken and the misuse alleged was not attributed to the person accused.

   c) Inquiry Investigation – Conducted by a member of the CLEAN Administrative Section to inquire if there is a violation of CLEAN/CJIS policies.

4) All agencies and agency personnel must cooperate with a CLEAN investigation or risk having their CLEAN privileges suspended or revoked.

   Note: Results of misuse investigations are reviewed by the CSO and CLEAN Administrative Section Supervisor for system integrity, security implication and for violation of these policies/procedures.

V) SYSTEM INTEGRITY, SUSPENSION AND REVOCATION OF ACCESS

1) The CSO or designee may suspend or revoke an operator's certification or individual's access for willfully or repeatedly violating these policies/procedures.

2) Upon suspension or revocation of an operator's certification or individual's access by the CSO or designee, written notice of the revocation or suspension shall be sent to the individual and to their agency administrator. The notice shall inform the parties of the decision and the procedure to request reconsideration. There are no individual rights of appeal.

3) An agency may terminate one of their personnel from CLEAN/CJIS access for cause. If an agency requests the CLEAN Administrative Section to remove an individual for reasons of misuse, the agency must make the notification in writing with the facts of the misuse and signed by the executive officer or their designee.

4) Individual discipline is a matter for the appropriate employing agency, and revocation or suspension of an individual's access to CLEAN is a decision taken separate and apart from agency action. The two are not related.

5) Access decisions are based on the necessity of ensuring the integrity of the CLEAN/CJIS information and system.

W) NOTICE OF VIOLATION BY AN AGENCY

1) Upon determination that a violation of this policy has occurred and that termination of an agency is appropriate, written notice of the violation shall be sent to the offending agency. The notice will contain the citation of the specific administrative policy/procedure alleged to have been violated and invite the agency to show just cause why total access should not be terminated by cancellation of the access agreement.

2) The offending agency must respond within 15 days of receipt of notification. The CLEAN Administrative Section will consider any material submitted, and determine what action best protects the integrity of the CLEAN/CJIS information and system. No individual or agency rights or privileges are involved in this matter. The only matters open for consideration, are the appropriateness of continued system access and if conditions on such access will ensure system integrity.

3) Reconsideration for an Agency

   a) If an agency and/or individual is found to be in violation of a Class 4 Offense and suspended or terminated, the agency may submit a request for reconsideration to the CJIS System Officer, within 15 days from the date of notification of violation. The decision of the CJIS System Officer is final.

   b) Remember, Class 1, 2 and 3 Offenses are NOT able to be reconsidered and are FINAL.

   c) All requests for reconsideration must be on agency letterhead and signed by the Chief Executive Officer for that agency. There is NO individual right or privilege granted for reconsideration.

4) No hearings are authorized. All submissions will be made in writing. All decisions will be delivered in writing.

   Note: Reference Appendix G: Sanctions Guide Lines

DEFINITIONS

The following definitions shall apply throughout these regulations:

Administration of Criminal Justice - The activities directly concerned with the prevention, control or reduction of crime; the apprehension, detention, pretrial release, post trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused persons or criminal offenders; criminal identification activities; or the collection, storage, dissemination, or usage of Criminal History Record Information (CHRI).

Administrative Message - A criminal justice related point-to-point free form message. This message may be asking for information or assistance, or it may be in response to a specific request from another agency. It is differentiated from other traffic in that it is free form and may be used for practically any type of official information transmission not associated with a specific message type.

Access – The term access as used in this regulation shall be defined as; opportunity to make use of an automated information system recourse. The ability to have contact with a terminal from which a transaction may be initiated.

Audit – An examination of an agency's records by an auditor from the CLEAN Administrative Section, Audit/Investigation Unit.

Authorized Agency - Any agency meeting the requirements for access to the CLEAN/CJIS system.

Authorized Personnel - Are those persons who have passed a state and national fingerprint-based record check and have been granted access to CLEAN systems and terminal areas.

Authorized User - An individual who has passed a state and national fingerprint-based record check and holds a current certification and has been authorized to access CLEAN/CJIS information.

Authorized Message – Messages that pertain to official agency matters and investigations.

Automated **F**ingerprint **I**dentification **S**ystem (AFIS) – The computer-based system for reading, encoding, matching, storage, and retrieval of fingerprint minutiae and images.

Bureau of **M**otor **V**ehicles, Pennsylvania Department of Transportation (BMV)

Criminal **J**ustice **I**nformation **S**ervices, Division of the FBI (CJIS)

CJIS Systems **A**gency (CSA)- Is a duly authorized state, federal, international, tribal, or

territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. The CSA is responsible for establishing and administering an IT security program throughout the CSA's user community, to include the local levels. There shall be only one CSA per state or territory. In Federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Officer (CSO)- An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network for the CJIS Systems Agency.

Central Repository - The central location for the collection, compilation, maintenance, and dissemination of Criminal History Record Information by the PSP (The Central Repository is the responsibility of the Bureau of Records and Identification within the PSP.

CLEAN Application – The user interface which provides access to CLEAN/NCIC.

CLEAN Investigation – An inquiry for ascertaining facts by the CLEAN Administrative Section, CLEAN Audit/Investigation Unit.

Code of **F**ederal **R**egulations (CFR) - Title 28, Code of Federal Regulations, Part 20.

Commonwealth **L**aw **E**nforcement **A**ssistance **N**etwork (CLEAN)- A statewide computerized information system established as a service to all criminal justice agencies – local, county, state, and federal – within the Commonwealth.

CLEAN/CJIS Security Policy - A document that includes the CJIS Security Policy and outlines specific technical security details that are associated with CLEAN connectivity.

Criminal **H**istory **R**ecord **I**nformation (CHRI)- information collected by criminal justice agencies concerning individuals and arising from the initiation of a criminal proceeding, consisting of identifiable descriptions, dates, and notations of arrests, indictments, information, or other formal criminal charges and any dispositions arising there-from. The term does not include intelligence information, investigative information, or treatment information, including medical and psychological information, or information and records specified in Section 9104 (relating to scope) of Pennsylvania Consolidated Statute, Title 18, Chapter 91, CHRI.

Computerized **C**riminal **H**istory **R**ecord **I**nformation (CCHRI)- is an electronic CHRI.

Control Terminal - NLB221 is the 24x7 control workstation for the CSA.

Criminal Justice Agency (CJA) - (1) courts; (2) a governmental agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice ('allocates a substantial part' has been interpreted to mean more than 50 percent by the originator of the Regulations). State and Federal Inspector General Offices are included.

Direct Access - Having the authority to access systems managed by PSP and the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency. This includes non 24 hour terminal agencies.

Direct Agency - An authorized agency that has the authority to access systems managed by PSP and the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

Disposition - Information indicating that criminal proceedings have been concluded, including information disclosing that police have elected not to refer a matter for prosecution, that a prosecuting authority has elected not to commence criminal proceedings, or that a grand jury has failed to indict and disclosing the nature of the termination of the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions of criminal proceedings in the Commonwealth shall include; but not be limited to, acquittal, acquittal by reason of insanity, pretrial probation or diversion, charge dismissed, guilty pleas, nolle prosequi, no information filed, nolo contendere plea, convicted, abatement, discharge under rules of the Pennsylvania Rules of Criminal Procedure, demurrer sustained, pardoned, sentence commuted, mistrial-defendant discharged, discharge from probation or parole or correctional supervision.

Dissemination - The oral or written transmission or disclosure of CHRI to individuals or agencies other than the criminal justice agency which maintains the information. (18 Pa.C.S. 9102).

Driver's License - A license or permit to drive a motor vehicle issued under Title 75.

Expunge - To remove information so that there is no trace or indication that such information existed; to eliminate all identifiers which may be used to trace the identity of an individual, allowing remaining data to be used for statistical purposes; or maintenance of certain information required or authorized under the provisions of Section 9122 (c) (relating to expungement) when an individual has successfully completed the conditions of any pretrial or post-trial diversion or probation program.

Full Access – Any workstation or device that can enter, modify, query and cancel in CLEAN/NCIC.

Full Access Certification –An individual who can enter, modify, query and cancel in CLEAN/NCIC.

Hardware - The physical terminal, computer equipment, devices, and peripheral equipment accessing CLEAN.

Hit Confirmation - Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions based upon the hit NCIC record: (1) arresting the wanted person, (2) detaining the missing person, (3) seizing the stolen property, or (4) charging the subject with violating a protection order. Additionally, an agency detaining an individual on local charges where the individual appears identical to the subject of the wanted person record *and is within the geographical area of extradition* must confirm the hit.

Hot Files – Any file which you can receive a response from.

Hot Sheets - The most recent report of CLEAN entries in the following categories: Wanted Persons-: last 48 hours, Missing Persons- last 48 hours. Stolen Vehicles- last eight hours. Philadelphia maintains a separate system.

.

Integrated **A**utomated **F**ingerprint **I**dentification **S**ystem (IAFIS)- Is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI). Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24/7 365 days a year.

Information **S**ecurity **O**fficer (ISO)- Is the CLEAN liaison to FBI CJIS Division on all technical security issues throughout the Commonwealth of Pennsylvania. All new network connections to CLEAN must be approved by the CLEAN ISO. All intrusions into an agency network must be reported to the CLEAN ISO for reporting to FBI CJIS Division.

Inappropriate Message - Any message that contains superfluous verbiage or embellishments or information of no value to the recipient; is unnecessary, excessive or abusive; or any other message that is not authorized.

Indirect Access - Access to the CLEAN/CJIS system through a direct access agency.

Indirect Agency – An agency who has access to the information from CLEAN/NCIC through an agency with direct access.

Interstate Identification Index – (III) - The FBI's automated system to provide an interstate exchange of criminal history information.

Interface - A method, either software or hardware, to communicate between two computers or computer systems.

Interface Agency - An authorized criminal justice or non-criminal justice agency which accesses CLEAN services through an established connection maintained by a CJA or NCJA with direct access to CLEAN services. The established CJA or NCJA is referred to as a "Direct Agency" and shall maintain a user agreement with the Interface Agency.

International Justice and Public Safety Information Sharing Network (Nlets)-- is a non-profit organization whose purpose is to provide interstate communications to law enforcement and criminal justice agencies.

Limited Access Workstation – Any terminal that can inquiry into CLEAN/NCIC only.

Limited Access Certification – A person that can inquiry into CLEAN/NCIC only.

LIVESCAN - Is a workstation capable of collecting and electronically transferring fingerprint and demographic (name, DOB, etc) data through the CLEAN to the PSP Criminal History Central Repository and the Federal Bureau of Investigation National Criminal History International Identification Index (III).

Local **A**gency **I**nformation **S**ecurity **O**fficer (LAISO) - Is designated by the local agency. The LAISO acts as the liaison between the local agency and ISO on all technical security issues, including the reporting of intrusions and vulnerabilities. Each agency that has direct access to CLEAN is required to have a LAISO assigned.

Management Control - The authority to set and enforce priorities, standards for the selection, supervision, and termination of personnel, and policy governing the operation of computers, or circuits, used to process, store, or transmit III record information and guarantees the priority service needed by the criminal justice community.

Metro - A server connected to CLEAN where devices are configured by the server agency, not by the CLEAN Administrative Section. Metros are responsible for their own policies and procedures which must meet or exceed CLEAN/CJIS requirements, including security, audits, logging, certification, etc.

Mobile **D**ata **C**omputer (MDC) - Allows access to CLEAN through computers permanently mounted in a vehicle.

National **C**rime **I**nformation **C**enter (NCIC) - NCIC stores vast amounts of criminal justice information which can be instantly retrieved by and/or furnished to any authorized agency. NCIC serves criminal justice agencies in the 50 states, the District of Columbia, Puerto Rico, and Canada.

Non-**C**riminal **J**ustice **A**gency (NCJA)- Any agency that does not meet the definition of a criminal justice agency in the Department of Justice Regulations on Criminal Justice Information Systems (Title 28, CFR, Part 20, Subpart A).

Non-**C**riminal **J**ustice **I**nformation (NCJI)- Is any message of a personal nature or a subject matter totally unrelated to the administration of criminal justice.

Non-Governmental Agency - Any agency that does not meet the definition of a Governmental Agency in the Department of Justice Regulations on Criminal Justice Information Systems (Title 28, CFR, Part 20, Subpart A).

Official Capacity - Users shall only utilize the data provided through CLEAN/CJIS systems in an official capacity of their criminal justice duties while conducting official criminal justice actions/investigations. Conducting any transactions while in an "off duty" status shall be scrutinized closely by the Local Agency Administrator and local policy should outline this specific use.

Official Record Holder – The Originating Agency that is responsible to maintain the original documentation and investigative supplements.

Operator Identifier - A unique identifier assigned to all certified operators used for gaining access to the CLEAN system.

Ordinance - A rule or law promulgated by a local or municipal governmental authority.

Originating **A**gency **I**dentifier (ORI) – The ORI is a unique nine-character identifier assigned by FBI CJIS Division staff to an agency which has met the established qualifying criteria for ORI assignment to identify the agency in transactions on the NCIC 2000 System.

Philadelphia Police department System (PCIC) – The Philadelphia Police Departments dedicated circuit to NCIC.

Portable Device – A device that can be hand-carried or easily moved (i.e., blackberry or laptop computer).

Private Agency - Any agency that has contracted with a government agency to provide services in connection with the administration of criminal justice.

PSP – (Pennsylvania State Police).

Recertification - Renewal of an operator's initial certification every 24 months.

Revocation - A permanent restriction on any access to CLEAN and CJIS systems and information, whether directly, indirectly or through a third party.

Right-to-Know - The right of an individual to inspect his or her own record.

Secondary Dissemination - The transfer of CCH/CHRI information to anyone legally entitled to receive such information that is outside the original requesting agency.

Secure Area - Any physical area established for CLEAN/NCIC operation, incorporating the use of a personal computer, database, server, printer, and any other related equipment and/or supplies.

Security Addendum- An official FBI document that outlines the requirements of vendors that require access to computers, networks or data that have access to or contains CJIS information. The vendor certification document is contained within the addendum. Each contract with vendors shall contain an indication to the existence of a security addendum.

Secure User Station - Any physical area established for CLEAN/NCIC operation, incorporating the use of a personal computer, database, printer, and any other related equipment and/or supplies.

Servicing Agreement - An agreement between a direct access agency and a indirect access agency to provide CLEAN services.

State - Any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

Statute - A law enacted by a state or federal legislative branch of government.

Supporting Documentation - Initial evidence that is required as proof or justification.

Switched Message – Is a message that may be used by CLEAN terminal personnel to exchange official information between law enforcement/criminal justice agencies.

Terminal **A**gency **C**oordinator (TAC) - The primary point of contact at the local level which serves as liaison between the CJIS Systems Officer and the local agencies that have access to a CSA criminal justice network. The responsibilities afforded to the TAC may vary from state to state.

Troop **C**ommunications **S**pecialist (TCS) - A person assigned to a PSP Troop to handle the duties and responsibilities of a TAC.

User Agreement - An agreement between a direct access agency and the CLEAN Administrative Section whereby the agency agrees to abide by all CLEAN/CJIS Regulations.

Validations - Obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active.

Vehicle Registration – The authority for a vehicle to operate on a highway as evidenced by the issuance of an identifying card and plate or plates.

Vendor - Any entity, by virtue of a contract or agreement, that provides any service to a criminal justice agency whereas the entity is a private (Non-Criminal Justice) agency and requires access to computer/network equipment that processes CJIS data or is connected to a CJIS network.

ACCRONYMS

AFIS – **A**utomated **F**ingerprint **I**dentification **S**ystem.

BMV – **B**ureau of **M**otor **V**ehicles, Pennsylvania Department of Transportation.

CJIS – **C**riminal **J**ustice **I**nformation **S**ervices, Division of the FBI.

CSA – **CJIS** Systems **A**gency.

CSO – **CJIS** Systems **O**fficer.

CLEAN – **C**ommonwealth **L**aw **E**nforcement **A**ssistance **N**etwork.

CHRI – **C**riminal **H**istory **R**ecord **I**nformation.

CCHRI – **C**omputerized **C**riminal **H**istory **R**ecord **I**nformation.

IAFIS – **I**ntegrated **A**utomated **F**ingerprint **I**dentification **S**ystem.

ISO – **I**nformation **S**ecurity **O**fficer.

III – **I**nterstate **I**dentification **I**ndex.

Nlets – International Justice and Public Safety Information Sharing Network.

LAISO – **L**ocal **A**gency **I**nformation **S**ecurity **O**fficer.

MDC – **M**obile **D**ata **C**omputer.

NCIC – **N**ational **C**rime **I**nformation **C**enter.

NCJA – **N**on-**C**riminal **J**ustice **A**gency.

NCJI – **N**on-**C**riminal **J**ustice **I**nformation.

ORI – **O**riginating **A**gency **I**dentifier.

PCIC – Philadelphia Police Department Circuit.

PSP – **P**ennsylvania **S**tate **P**olice.

TAC – **T**erminal **A**gency **C**oordinator.

TCS – **T**roop **C**ommunications **S**pecialist.

APPENDIXES

A **Audit/Investigation Manual**

Details the audit process and how CLEAN investigations shall be conducted.

B. **Hit Confirmation Manual**

Details the processes and procedures for HIT confirmations.

C. **Information Security Policy Manual**

Details the security procedures / policies for the CLEAN system.

D. **Obtaining an ORI**

Details the procedure to obtain and ORI.

E. **Operator Certification Procedures**

Details the procedure on certifying a CLEAN operator.

F. **PSP Use of JNET**

Details PSP use of JNET.

G. **Sanction Guidelines Manual**

Details the CLEAN system misuse violations and sanctions.

H. **Terminal Agency Coordinator (TAC) Manual**

Details the rules, procedures and policies for the TAC officer.

I. **Validation Manual**

Details the processes and procedures for validations of the CLEAN/CJIS systems.