pennsylvania
OFFICE OF STATE
INSPECTOR GENERAL

POLICY

CLEAN/NCIC ACCESS AND USE

Date: August 30, 2021	By Direction Of: Lucas M. Miller, State Inspector General

A. Purpose & Scope.

To define the Office of State Inspector General's (OSIG) policy and procedures regarding usage of the Commonwealth Law Enforcement Assistance Network (CLEAN), and the National Crime Information Center (NCIC) database. This policy applies to all OSIG employees. Failure to abide by this policy may result in disciplinary action up to and including termination.

The successful completion of the qualification steps as well as obtaining and maintaining access to these databases is a requirement of employment for OSIG sworn law enforcement staff.

B. Definitions.

Commonwealth Law Enforcement Assistance Network (CLEAN) – A statewide computerized information system established as a service to all law enforcement and criminal justice agencies within the Commonwealth of Pennsylvania. CLEAN is administered by the Pennsylvania State Police (PSP).

Criminal History Record Information (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 therefrom. 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 of the Criminal History Record Information Act ("Act"), adopted in January of 1980.

Criminal History User (CH) – provides the user access to all criminal justice information available within JNET, but not Pennsylvania State Police (PSP) Computerized Criminal History Record Information (CCHRI). This is the default setting for JNET users who belong to a Criminal Justice or Law Enforcement Agency before they complete CLEAN Certification. Users requesting access to this role must work for a criminal justice agency as defined by CHRIA.

Dissemination – the oral, written, or electronic transmission or disclosure of criminal history record information to individuals or agencies other than the criminal justice agency which maintains the information.

Interstate Identification Index (III) – Contains personal descriptive information that an authorized agency can use to determine if a subject has a state or federal criminal history record on file. The III is not an NCIC file but is an index accessible through the NCIC system.

National Crime Information Center (NCIC) – The United States' central database for tracking crime-related information. It is maintained by the Criminal Justice Information Services Division (CJIS) of the Federal Bureau of Investigation (FBI) and is interlinked with federal, tribal, state, and local agencies and offices.

National Law Enforcement Telecommunications Systems (NLETS) – NLETS is an information sharing network which allows a law enforcement agency in one state to query another state's criminal and driver records.

Secondary Source Verification – Additional independent confirmation of information obtained through CLEAN/NCIC.

Terminal Agency Coordinator (TAC) – The TAC is responsible for approving and coordinating access to the CLEAN/NCIC databases. The TAC serves as the liaison between the OSIG and the Pennsylvania State Police (PSP) CJIS Systems Officer.

C. Policy.

All information defined above as CHRI is covered under the Criminal History Record Information Act (CHRIA). CHRIA provides for an orderly collection and dissemination of criminal history information in the Commonwealth of Pennsylvania and sets forth security parameters for the storage and dissemination of information. All OSIG employees must follow the directives outlined below concerning the access, collection, recording and dissemination of CHRI information. These databases are to be used only during the course of an employee's official OSIG duties.

All OSIG employees, including those who will not be accessing the CLEAN/NCIC databases, are required to be fingerprinted and complete the Criminal Justice Information Services (CJIS) online security awareness training.

CLEAN/NCIC users are responsible for reading, understanding, and complying with all CLEAN/NCIC policies and procedures.

D. Data Registration.

CLEAN/NCIC is a restricted database which requires the completion of certain qualification steps to ensure proper compliance with mandated state and federal government standards.

All initial and ongoing access to the CLEAN/NCIC databases will be coordinated by the OSIG's Terminal Agency Coordinator (TAC).

An authorized and active JNET Criminal Justice (CJ) account is necessary to request the Criminal History (CH) role. This CH role is required to access CHRI information and also to gain entry to the PSP CLEAN PortalXL application which allows direct access to CLEAN/NCIC databases.

The following additional steps are necessary for the OSIG employee to obtain certification allowing access to the CLEAN/NCIC databases and CHRI:

1. If an OSIG employee has not been properly fingerprinted and provided the TAC a copy of their fingerprint card, that employee will need to do so before continuing.
2. The OSIG employee will utilize the JNET User Provisioning System to request the Criminal History (CH) role.
3. The OSIG employee with the Criminal History (CH) role will utilize JNET to gain access to the PSP CLEAN PortalXL application.
4. The OSIG employee uses the CJIS Online hyperlink to complete the security awareness and local operator training, followed by a final exam.
5. The OSIG employee must satisfactorily pass the operator training exam to maintain access to CLEAN/NCIC databases.
6. The OSIG employees are required to complete re-certification every two years after receiving email notification from PSP/CLEAN.

CLEAN/NCIC Information Search Log Procedures

All users, after conducting a search of the CLEAN/NCIC database, must complete the online Information Search Log in a timely manner after every inquiry they make. On the last business day of the month, JNET automatically sends each user's Information Search Log to the JNET Terminal Agency Coordinator (JTAC). If a user conducts no activity in CLEAN during the month, the user must complete a "no activity" entry in the Information Search Log by the last business day of the month in order for JNET to submit the user's JNET Information Search Log to the JTAC. Click here for instructions on completing the online Information Search Log. Non-compliance will result in notification(s) from JNET to the violating user and their direct supervisor. When notified of an employee's violation(s), the supervisor will ensure the employee's understanding of this policy and his/her compliance with the policy going forward. If compliance is not achieved, both the violating user and their direct supervisor may be subject to disciplinary action and the potential loss of JNET access.

E. Usage of CLEAN/NCIC Information

OSIG sworn law enforcement staff, and certain other designated staff who are authorized by their Criminal History (CH) user role may query the CLEAN/NCIC database. All inquiries entered into the system and any information accessed/retrieved **must** be related to an official OSIG investigation.

Bureau of Fraud Prevention and Prosecution (BFPP) staff will use information obtained through CLEAN/NCIC as a lead for secondary source verification, except for certified Pennsylvania Department of Transportation (PennDOT) information. The release of printed CLEAN/NCIC screens is prohibited; however, the secondary source verification information can be released to a third party, provided its release does not violate existing OSIG policy. BFPP staff can use only PennDOT photographs for identification purposes after removing personal information related to the photograph. The source of the photograph cannot be revealed to a third party. Photographs obtained from PennDOT may not be disseminated to the media and must be destroyed at the conclusion of an investigation, after all appeals have been exhausted. Information obtained from PennDot may not be uploaded to the digital case file. Certified PennDOT information can be stored with the investigation and retained and purged per the OSIG Record Retention Schedule. All other relevant PennDot information should be transcribed in the OSIG 10 (Investigation Case Notes), the OSIG 11 (Report of Investigation) or the OSIG 611 (Investigative Activity Summary). Photographs from WebCPIN are to be used in any published materials (ex: press releases). All other CLEAN/NCIC information, outside of PennDot information, will be retained and purged per the OSIG Record Retention Schedule.

Bureau of Special Investigations (BSI) staff may use Criminal History information as a source during background investigations for law enforcement positions (Troopers, OSIG Sworn Law Enforcement Staff, and other law enforcement titles). CH information will not be used for non-law enforcement positions in a law enforcement/criminal justice agency. For example, it should not be used for a clerical or administrative position within a law enforcement agency, such as a receptionist. BSI staff will upload relevant non PennDOT CLEAN/NCIC information into the case record located in their Case Management Tracking System (CMTS) or will document in the Case Notes Section within Details the fact that no relevant information was found through a CLEAN/NCIC inquiry. Non PennDOT information obtained from CLEAN/NCIC will be retained and purged per the OSIG Record Retention Schedule.

Bureau of Law Enforcement Oversight (BLEO) staff will use information obtained through CLEAN/NCIC as a lead for secondary source verification, except for certified Pennsylvania PennDOT information. The release of printed CLEAN/NCIC screens is prohibited; however, the secondary source verification information can be released to a third party, provided its release does not violate existing OSIG policy. BLEO staff may be provided CLEAN/NCIC information from law enforcement during the course of a review. Information provided to BLEO does not have to be logged into the JNET/CLEAN/NCIC Search Log. BLEO staff can use only PennDOT photographs for identification purposes after removing personal information related to the photograph. The source of the photograph cannot be revealed to a third party. Photographs obtained from PennDOT may not be disseminated to the media and must be destroyed at the conclusion of an investigation, after all appeals have been exhausted.

Information obtained from PennDot may not be uploaded to the digital case file. Certified PennDOT information can be stored with the investigation and retained and purged per the OSIG Record Retention Schedule. All other relevant PennDot information should be transcribed into CMTS. Photographs from WebCPIN are to be used in any published materials (ex: press releases). All other CLEAN/NCIC information, outside of PennDot information, will be retained and purged per the OSIG Record Retention Schedule. BLEO staff will upload relevant non PennDOT CLEAN/NCIC information into the case record located in their Case Management Tracking System (CMTS) or will document in the Case Notes Section within Details the fact that no relevant information was found through a CLEAN/NCIC inquiry.

All OSIG personnel are responsible to immediately report any unauthorized physical or electronic access of the CLEAN/NCIC databases or information to the OSIG's Terminal Agency Coordinator (TAC).

F. CLEAN/NCIC Security

CLEAN/NCIC database users must protect their system passwords. Users must not disclose or allow another to use their password to access these databases. Users must always log off the CLEAN/NCIC database before leaving the work area. Unauthorized CLEAN/NCIC use, disclosure of a password, or misuse of CLEAN/NCIC information may result in disciplinary action up to and including termination, civil proceedings, or criminal penalties.

G. CLEAN Administrative Roles

TAC

The TAC is the liaison between the OSIG and the Pennsylvania State Police (PSP) CJIS Systems Officer. The TAC is responsible for approving and coordinating access to CLEAN/NCIC databases. This includes maintaining each employee's CLEAN Operator file, which includes: copies of the employee's fingerprints, results and date of the last certification/recertification exam, and the results of the last background check. Additionally, the TAC is responsible for ensuring compliance with CLEAN/NCIC and National Law Enforcement Telecommunications Systems (NLETS) policy and regulations relative to:

- Attending user group meetings conducted by PSP.
- Validation Requirements.
- Proper System Usage.
- Operator Certification Testing.
- Assisting CLEAN/NCIC audit staff.
- Assisting on any investigation of system misuse or improper operator procedures upon request.
- Instructing members on system security and training of new users.
- Any additional duty that may be required or requested to maintain the integrity and security of the system.

All accounts shall be reviewed at least every six months by the TAC or his/her designee to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC will also modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc., and cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

Per PSP policy, the TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) shall be suspended. For OSIG employees suspended as part of the disciplinary process, his/her manager must notify the TAC. The TAC will suspend the employee's CLEAN/NCIC access for the duration of the suspension.

> **NOTE:** Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated supervisor or manager.

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.).

H. Dissemination.

The dissemination of CLEAN/NCIC information will follow CLEAN/NCIC dissemination guidelines. Specifically, CLEAN/NCIC mandates documentation on a dissemination log for any secondary dissemination of any III/CHRI to any criminal justice agency, or an individual within another criminal justice agency, or to anyone legally entitled to receive such information outside the original receiving agency. The III/CHRI dissemination log shall be maintained for at least 12 months and such be available for audit.

I. Auditing.

The use of CHRIA protected information from the CLEAN/NCIC databases will be audited every two years by the Pennsylvania Office of Attorney General (OAG) and every three years by PSP. The TAC is responsible to coordinate and assemble all records as requested by the OAG and PSP.

The Commonwealth's policy regarding JNET may be found in Management Directive 245.16 Amended, Pennsylvania Justice Network (JNET) Governance Structure. Additional JNET policies can be accessed through the Commonwealth of Pennsylvania Justice Network.

J. Additional Information.

Any questions regarding this policy should be directed to your supervisor.