pennsylvania
OFFICE OF STATE
INSPECTOR GENERAL

POLICY

JNET 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 Pennsylvania Justice Network (JNET). 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 this database is a requirement of employment for OSIG sworn law enforcement staff.

B. Definitions.

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 (CHRIA), adopted in January of 1980 (18 Pa. C.S.A. §9101 et seq.).

Criminal History User (CH) – provides the user access to all criminal justice information available within JNET, but not Pennsylvania State Police 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.

JNET Registrar - The JNET Registrar is responsible for maintaining roles and JNET access within the User Provisioning System and performing annual Pennsylvania Department of Transportation (PennDOT) transaction audits of all users.

JNET Security Administrator – The main responsibility of the JNET Security Administrator is to investigate user misuse of JNET. The other roles include performing audits and writing JNET policies.

JNET Sponsor – The role of the JNET Sponsor is to oversee those individuals applying for access to JNET.

Justice Terminal Agency Coordinator (JTAC) – the liaison between the OSIG and JNET. The JTAC is responsible for coordinating initial and ongoing access for OSIG users.

Pennsylvania Justice Network (JNET) – The integrated justice portal provides a common online 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. JNET will be the portal normally used by OSIG employees to access CLEAN/NCIC and other databases.

Secondary Source Verification – Additional independent confirmation of information obtained through JNET.

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 performance of an employee's official OSIG duties.

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

JNET users are responsible for reading, understanding, and complying with the JNET User Agreement, which contains the User Roles and Secured Applications, User Terms and Conditions. New JNET users must digitally sign the JNET User Agreement Form; JNET users who registered prior to 2010 must have a signed hardcopy of the JNET User Agreement Form on file with the JNET Registrar.

D. Database Registration.

JNET 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 JNET database will be coordinated by the OSIG's Justice Terminal Agency Coordinator (JTAC).

User Registration Procedures

OSIG employees authorized to access the JNET database to secure information needed in the course of conducting their ***official*** OSIG duties and who are **not already JNET users** must follow the registration procedures below.

1. All new JNET accounts will be created through a Sponsor invitation. Users will no longer be able to self-register for accounts that require subsequent Sponsor approval.
2. From the IGNet, click on the BFPP page. On the BFPP page, click on the Forms dropdown arrow, select *JNET Forms*, and click *Go*. Click and open the OSIG JNET Information Request Log Memorandum.
3. Read, print, date, and sign the OSIG JNET Information Request Log Memorandum and e-mail it to the JNET Registrar. **This form must be completed and received by the JNET Registrar before you will be approved for JNET access**.
4. JNET Sponsors will generate "New User Invitations" within the JNET User Provisioning System.
5. After the Sponsor enters and submits the new user's demographic and organizational information, an email will be automatically generated and sent to the new user inviting them to enroll for JNET access.
6. Upon receipt of the invitation, the new user will select the link which directs them to the JNET Internet Site to complete the registration process.
7. In order for the new user to confirm their identity and complete the registration process, they will be required to enter an activation and security code that is provided by JNET in the emailed user invitation.

   NOTE: When completing the Registration Form, place the appropriate regional office address in the Organization Location Block.
8. Users will be responsible for completing the registration process within 15 days of issuance of the invite or the invitation will be cancelled.
9. New users will continue to acknowledge the JNET Security Policy, create a password, answer challenge questions, and complete JNET Overview Training.
10. Upon receipt of your individual user identification and password, access JNET LMS Training, click on the Training Link located on the right-hand side of the web page, follow the instructions, and complete the training.
11. Linked is the New User Quick Reference Card that provides an overview of the process new users will follow.
12. At the completion of this stage, the OSIG employee will be granted access as a Criminal Justice (CJ) user.

NOTE: The new user registration process will only be available on the JNET Internet Site (www.jnet.pa.gov).

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 to gain entry to the PSP CLEAN PortalXL application which allows direct access to CLEAN/NCIC databases.

JNET Information Search Log Procedures

All users must complete the online Information Search Log in a timely manner after every inquiry made to a JNET database. If a user conducts no activity in JNET 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 JNET 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 JNET Information.

OSIG sworn law enforcement staff, and certain other designated staff who are authorized by their Criminal History (CH) user role may query JNET. 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 JNET/CLEAN/NCIC as a lead for secondary source verification, except for certified Pennsylvania Department of Transportation (PennDOT) information. The release of printed JNET/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 JNET 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 JNET 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 JNET inquiry. Non PennDOT information obtained from JNET will be retained and purged per the OSIG Record Retention Schedule.

Bureau of Law Enforcement Oversight (BLEO) staff will use information obtained through JNET/CLEAN/NCIC as a lead for secondary source verification, except for certified PennDOT information. The release of printed JNET/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 JNET/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 JNET information, outside of PennDot information, will be retained and purged per the OSIG Record Retention Schedule. BLEO staff will upload relevant non PennDOT JNET 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 JNET inquiry.

All OSIG personnel are responsible to immediately report any unauthorized physical or electronic access of the JNET databases or information to the OSIG's JTAC.

F. JNET Security.

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

G. Dissemination.

The dissemination of JNET information will follow JNET's dissemination guidelines.

H. Auditing.

The JTAC will conduct quarterly JNET audits to ensure compliance and security integrity with JNET and OSIG policy.

PennDOT driver's record information obtained from JNET will be internally audited annually by the OSIG's JNET Registrar.

The overall usage of JNET resources will be audited by the JNET Security Administrator every three years. The JTAC is responsible to coordinate and assemble all records as requested by the JNET Security Administrator.

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.

I. Additional Information.

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