POLICY STATEMENT
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Centralized Clearances		**1.1.4**
Date of Issue:	**Authority:**	**Effective Date:**
February 6, 2023	**Signature on File** **Dr. Laurel R. Harry**	**February 13, 2023**

I. AUTHORITY

The Authority of the Secretary of Corrections to direct the operation of the Department of Corrections is established by Sections 201, 206, 506, and 901-B of the Administrative Code of 1929, 71 P.S. §§61, 66, 186, and 310-1, Act of April 9, 1929, P.L. 177, No. 175, as amended.

II. APPLICABILITY

This policy is applicable to all facilities operated under the jurisdiction of, or conducting business with the Department of Corrections, Department employees, volunteers, contract personnel, visitors and inmates.

III. POLICY

It is the policy of the Department to ensure the security of the National Crime Information Center/Commonwealth Law Enforcement Assistance Network/Pennsylvania's Justice Network (NCIC/CLEAN/JNET) Systems and that staff comply with Federal, State, and statutory regulations. To ensure the safety and security of all Department facilities, as well as the community, the Department shall monitor the access of all individuals and the egress of all inmates from its facilities. This monitoring includes all information available through the NCIC/CLEAN/JNET Systems or any other electronic informational database.

IV. PROCEDURES

All applicable procedures are contained in the procedures manual that accompanies this policy document.

V. SUSPENSION DURING AN EMERGENCY

In an emergency or extended disruption of normal facility operation, the Secretary/designee may suspend any provision or section of this policy for a specific period.

VI. RIGHTS UNDER THIS POLICY

This policy does not create rights in any person nor should it be interpreted or applied in such a manner as to abridge the rights of any individual. This policy should be interpreted to have sufficient flexibility to be consistent with law and to permit the accomplishment of the purpose(s) of the policies of the Department of Corrections.

VII. RELEASE OF INFORMATION AND DISSEMINATION OF POLICY

A. Release of Information

1. Policy

   This policy document is public information and may be released upon request.

2. Confidential Procedures (if applicable)

   Confidential procedures for this document, if any, are not public information and may not be released in its entirety or in part, without the approval of the Secretary of Corrections/designee. Confidential procedures may be released to any Department of Corrections employee on an as needed basis.

B. Distribution of Policy

1. General Distribution

   The Department of Corrections policy and procedures shall be distributed to the members of the Central Office Executive Staff, all Facility Managers, and Community Corrections Regional Directors on a routine basis. Distribution of confidential procedures to other individuals and/or agencies is subject to the approval of the Secretary of Corrections/designee.

2. Distribution to Staff

   It is the responsibility of those individuals receiving policies and procedures, as indicated in the “General Distribution” section above, to ensure that each employee expected or required to perform the necessary procedures/duties is issued a copy of the policy and procedures either in hard copy or via email, whichever is most appropriate.

VIII. SUPERSEDED POLICY AND CROSS REFERENCE

A. Superseded Policy

1. Department Policy

   1.1.4, issued September 29, 2014, by former Secretary John E. Wetzel.

2. Facility Policy and Procedures

   This document supersedes all facility policy and procedures on this subject.

B. Cross Reference(s)

1. Administrative Manuals

   a. 1.1.6, Volunteers and Interns in the Department of Corrections

   b. 4.1.1, Human Resources and Labor Relations

   c. 6.3.1, Facility Security

   d. 11.5.1, Records Office Operations

2. ACA Standards

   a. Adult Correctional Institutions: 5-ACI-1F-08

   b. Adult Community Residential Services: None

   c. Correctional Training Academies: None

3. PREA Standards

   115.17

PROCEDURES MANUAL
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Centralized Clearances		**1.1.4**
Date of Issue:	**Authority:**	**Effective Date:**
February 6, 2023	**Signature on File** **Dr. Laurel R. Harry**	**February 13, 2023**

Release of Information:

Policy Document: This policy document is public information and may be released upon request.

Procedures Manual: The procedures manual for this policy may be released in its entirety or in part, with the prior approval of the Secretary/designee. Unless prior approval of the Secretary/designee has been obtained, this manual or parts thereof may be released to any Department employee on an as needed basis only.

Section 1 – Systems Use and Security

Section 2 – Information Requests and Dissemination

Section 3 – Retention and Expungement

Section 4 – Centralized Clearance Check Procedures

Section 5 – NCIC/CLEAN/JNET

Section 1 – Systems Use and Security

A. General

National Crime Information Center/Commonwealth Law Enforcement Assistance Network/Pennsylvania's Justice Network (NCIC/CLEAN/JNET) systems shall be accessed by trained personnel who requires this access for the routine operations of their position. Information shall be utilized for official purposes and shall be disseminated to Department staff who have a legitimate need-to-know/right-to-know, and shall not be disseminated to any outside source, unless shared with another criminal justice agency during the course of an official investigation/proceeding. Protected or restricted information must be secured according to statute and policy.

B. Systems Use

1. Inmates – Systems shall be queried to determine existing criminal history, disposition of charges, outstanding warrants, detainers, extradition and any other relevant information as required in accordance with Department policy **11.5.1, "Records Office Operations."**

2. Inmate Visitors – Systems may be routinely accessed to assist in the identification or approval of visitors on the inmate's visitation list.

3. Employment – Systems shall be accessed to determine the suitability of potential employees and/or the continuation of employment, i.e., promotion, transfer, internal investigation, etc.

4. ***Non-Departmental Staff Access Requests*** – ***System access is to determine approval for issuing the security clearance of those who may enter or conduct business in a Department facility.***

5. Investigations – Systems may be accessed during the course of any inquiry, formal or information, into criminal/administrative incidents or allegations of criminal/administrative wrongdoing.

C. Systems Security

1. The data stored in and available through the NCIC/CLEAN/JNET systems or related electronic informational databases, is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. The systems must be secure from <u>any</u> unauthorized use. Non-public criminal history information or restricted information obtained through these systems may not be transmitted through non-encrypted electronic transfer. An audit trail must be implemented for all criminal history information extracted from NCIC/CLEAN/JNET. Each Facility Manager shall ensure that only trained and certified operators are authorized direct access to these systems. Only those Department personnel who have met all state/federal requirements shall have indirect access to restricted information obtained directly from these systems.

Issued: 9/29/2014
Effective: 10/27/2014

2. The data stored and available through NCIC/CLEAN/JNET is **CONFIDENTIAL** and must be treated accordingly. Any unauthorized request or receipt of restricted material could result in administrative, civil, or criminal proceedings.

3. NCIC/CLEAN/JNET information may only be secondarily disseminated to another authorized Criminal Justice Agency on a right-to-know/need-to-know basis, **for official purposes only**, and only when in conjunction with a joint investigation. Release of any information secondarily disseminated to another Criminal Justice Agency during the course of a joint investigation must be documented.

4. Criminal history extracted from these systems may never be disseminated to any non-criminal justice agency or individual. Destruction records will be maintained for all CHRI extracted from the system.

5. Questions relating to the operation of NCIC/CLEAN/JNET, policy modifications or dissemination of this computerized information shall be directed to the Central Office System Agency Coordinator/JNET System Agency Coordinator (TAC/JTAC).

6. Each facility shall designate a CLEAN/JNET Field Coordinator as the liaison to the TAC/JTAC for NCIC/CLEAN/JNET operations. ***An alternate Field Coordinator is also suggested. These individuals must be experienced certified CLEAN and JNET operators who will be responsible for on-site training, testing and troubleshooting.***

7. Each facility shall maintain a sufficient number of certified operators to ensure 24-hour coverage for the Control area, as well as normal operational routine of the facility.

Section 2 – Information Requests and Dissemination

A. Information Requests

The NCIC/CLEAN/JNET systems shall be queried as part of this process to determine suitability of all potential Department employees and ***non-department individuals requesting access into Department facilities.*** The system may also be used in subsequent instances of investigation, review, promotion, transfer, etc.

1. The facility Human Resource Office is responsible for the initial background

2. All requests for Centralized Clearances ***for a single facility*** are the responsibility of the facility Security Office, which may be supplemented by the Centralized Clearance Unit (CCU).

3. ***Clearances for the PA Prison Society, Pennsylvania Board of Probation and Parole (PBPP), contract service providers and agency temps will be the responsibility of the CCU.***

4. ***Clearances for Central Office projects may be submitted to CCU directly through the respective Bureau's designated liaison.***

5. Request for routine inmate information is the responsibility of the Inmate Records Office.

6. All other requests for restricted or protected information from NCIC/CLEAN/JNET systems must be pre-approved by an authorized source and only in conjunction with an official purpose. ***These requests should be submitted to the local facility Security Office or the CCU.***

B. Dissemination of Information

1. The Records Office is responsible for the dissemination of all facility requests for NCIC/CLEAN/JNET information extracted from the **DC-15**. Dissemination of information is the oral, written, or electronic transmission or disclosure of restricted/protected/criminal history information extracted from the NCIC/CLEAN/JNET System. This information shall be used by the Department for official purposes only. Any secondary dissemination of this information to a non-criminal justice agency or individual is strictly prohibited. Secondary dissemination includes, but is not limited to, visual, oral, electronic or written transmission of this information. Secondary dissemination of this information shall be logged on the **Inmate Dissemination Sheet (Attachment 2-A, Page 1)** for control purposes, when queried and/or destroyed.

2. ***Secondary dissemination for all others will be the responsibility of the respective office and shall be logged on the Non-Inmate Dissemination Sheet (Attachment 2-A, Page 2).***

Issued: 9/29/2014
Effective: 10/27/2014

3. Any individual who is requesting copies of his/her own criminal history records to determine completeness and accuracy, or for a non-Department official purpose shall be referred to the Pennsylvania State Police (PSP) Repository via PSP form **SP 4-164, Request for Criminal Record Check (Attachment 2-B)**.

4. Maintenance of dissemination/destruction logs for all ***secondary dissemination requests*** from these systems is the sole responsibility of the ***individual who is providing this information***. These individuals are responsible for all security and expungement requirements.

C. Reproduction of NCIC/CLEAN/JNET Information

1. Inmate Records

   a. The Records Office is responsible for the reproduction of all facility requests for NCIC/CLEAN/JNET information for an inmate. A dissemination sheet shall be appended to each **DC-15** in the Identification Section.

   b. Secondary dissemination of this information is prohibited without notification to the Records Office. All reproduced copies of Criminal History Record Information Act (CHRIA) information shall also be stamped in red with the official designated disclaimer and logged as required.

2. General

   Criminal history inquiries conducted on non-inmates shall be documented in compliance with the rules of dissemination/destruction. Responsibilities shall include appropriate security, logging, and disposal requirements.

Issued: 9/29/2014
Effective: 10/27/2014

Section 3 – Retention and Expungement

A. Retention of Information

1. Inmate Records

   The **DC-15** shall contain the most recent criminal history record available on the inmate. ***Actual copies of an inmate's RAP sheet should not be retained within the DC-15.***

2. Human Resources

   For those candidates appointed to positions within the Department, the original NCIC/CLEAN/JNET inquiry responses shall be forwarded with the employment package to the Central Office Bureau of Human Resources (BHR) for processing and retention. ***Staff or candidate queries should be conducted using the purpose code "J" for criminal justice employment.*** The facility shall not retain copies. Criminal history information extracted from these systems and incorporated into reports of any form will not be disseminated to a non-criminal justice agency.

3. Security (Facilities)

   When conducting centralized clearance checks for security suitability, the original response shall be retained until determination of approval/disapproval is made. This electronic response to the NCIC/CLEAN/JNET inquiry shall then be destroyed. Criminal history responses generated as the result of an official investigation may be retained pending the conclusion of the investigation and the disposition of all charges. The NCIC/CLEAN/JNET response shall be destroyed when the information is no longer relevant or necessary to the goals and objectives of the investigation or the agency.

4. Central Office/Community Corrections Centers (CCCs)/Training Academy/Community ***Contract Facilities (CCFs)***

   Criminal history inquiry response maintained by Central Office/CCCs/Training Academy/***CCFs*** may be retained until the data is no longer relevant or necessary to the goals and objectives of the Department, the data has become obsolete making it unreliable for present purposes, or the data cannot be used for strategic or tactical intelligence purposes. All queries, dissemination, and destruction of information shall be documented according to state/federal regulations, Department policy, and PA statute. ***Only those individuals within CCFs who have been fingerprinted and cleared for Criminal History access to information extracted from these systems, shall be eligible to review this information.***

B. Expungement

1. Upon receipt of official notification of expungement, the Department shall remove any evidence of said criminal history from Department documents. This expungement order

Issued: 9/29/2014
Effective: 10/27/2014

shall be forwarded to all agents who were recipients of this disseminated information. Once the information is expunged, the expungement order shall be destroyed.

2. Responsibilities include appropriate security, logging, and disposal requirements.

Section 4 – Centralized Clearance Check Procedures

A. Candidate

1. The candidate (civilian who is requesting clearance) is responsible for completing **Section A** on the **Centralized Clearance Check Information Request Form (Public)** ***(Attachment 4-A)*** which is available on the Department's public website (www.cor.pa.gov). Third parties may not complete forms on the candidate's behalf without the candidate's validation of the final document. If additional space is needed, the candidate may use additional paper. All fields in **Section A** shall be completed by the candidate including his/her social security number. If the candidate has not been issued a social security number, he/she may provide another form of federal identification information such as a passport, visa, or alien registration information. If particular information does not apply to the candidate, the candidate should indicate N/A in the applicable section of the form. Omission of pertinent information or the falsification of information shall be grounds for immediate disapproval ***or possible criminal prosecution***.

2. A clearance is only valid for a maximum of 24 months for volunteers, agency temps, mentors, reentry service providers, contract service providers, ***official visitors, public visitors, interns, organizations, Vendor I and Vendor II***. ***Clearances may be issued for shorter periods and*** the length of any clearance approval should always represent the period that the individual actually requires access. **(28 C.F.R. §115.17 [e] Contractors)**

3. It is the responsibility of the candidate to renew his/her clearance before its expiration. For those individuals who have been issued a Department photo ID, the expiration of his/her clearance or photo ID will result in an alert being generated on the biometrics front panel during the check-in process. ***The candidate is required to provide the updated Centralized Clearance Check Information Request Form (Public) to the requestor three weeks prior to his/her clearance expiration***.

4. All non-Department staff must have an active clearance before they are issued/reissued a Department photo ID.

5. ***All clearances will be a statewide clearance unless documented otherwise in the centralized clearance system. A candidate may be excluded from visiting a certain facility where any inmate(s) are housed and with whom they have had recent communications with. These communications would include an active visitor or communications via telephone calls, emails, mail, and/or monetary transactions within one year of the clearance request***.

6. The **Centralized Clearance Check Information Request Form (Public)** contains a signature line in which the candidate acknowledges that he/she completed the form, agrees that the information contained in the application is accurate, and agrees that he/she assumes all risks and liabilities associated with entering the applicable facility or

facilities. ***Any falsified information will be grounds for a clearance disapproval or possible criminal prosecution***.

NOTE: Any civilian who has been granted a clearance to access a facility, through the centralized clearance process, shall assume all risks associated with entering the applicable facility. ***Individuals with limited access*** shall be supervised ***and escorted*** by Department staff at all times while in a Department facility ***or when outside the secure perimeter***. ***Following the security orientation, individuals with full access do not require supervision or an escort throughout the facility***.

7. Full disclosure of all relationships with inmates confined in any Department facility is required. Such disclosable relationships with inmates shall include, but are not limited to, ***an active inmate visitor,*** money transactions, ***or communication via telephone calls, mail, or email***.

8. Completed forms should be hand delivered, mailed, or sent via email to the Department staff requestor for review and submission to the facility Security Office or the Centralized Clearance Unit (CCU).

B. Requestor

The requestor is an authorized Department staff member who is ***requesting*** the candidate's clearance request. Non-Department staff may not act as requestors. ***A clearance is only required for reoccurring access. A requestor requesting a one to two day access or access for a current Commonwealth employee should contact the facility Security Office in accordance with Department policy 6.3.1, "Facility Security," Section 31***.

1. ***A facility*** requestor's responsibilities include the following:

   a. informing the candidate that the **Centralized Clearance Check Information Request Form (Public)** is available on the Department's public website at www.cor.pa.gov;

   b. reviewing **Section A** of the form ***for any incomplete/illegible fields. No spaces should be blank and if a question does not apply to the candidate, "Not Applicable (N/A)" should be entered in the appropriate space. If any incomplete/illegible fields are identified, the form will be returned to the candidate for verification of the information in question and the approval process will be delayed as a result***;

   c. completing **Section B** on the **Centralized Clearance Check Information Request Form (Public)** (This section of the form must be completed in its entirety and the nature of the access ***is*** required ***[full or limited]***). The requestor should also indicate if there are special provisions applicable to the candidate such as "outside secured perimeter only." (The inclusion of specific documentation in **Section B** by the requestor will help to expedite the clearance approval process for the approving authority);

Issued: 4/30/2018
Effective: 5/23/2018

d. ***sending a PREA Current/Prior Employer Letter, if applicable, as outlined below in Subsection C.3. and in accordance with Department policy 4.1.1, "Human Resources and Labor Relations," Section 40;***

e. forwarding all **Centralized Clearance Check Information Request Forms (Public)** to the ***requestor's home*** facility Security Office ***two weeks prior to the requested access begin date or clearance expiration date. Requests to expedite a clearance will be considered on a case by case basis***. (**Section B** must be completed by the requestor or the form will not be processed. The requestor should not retain personal copies of submitted forms); and

f. notifying the facility Security Office when a clearance should be inactivated due to voluntary separation or loss of privileges. (The clearance and any issued Department photo ID must be deactivated.)

2. ***A Central Office requestor's responsibilities include Subsection B.1.a. through d. above, along with the following:***

a. ***forwarding all Centralized Clearance Check Information Request Forms (Public) to the CCU one week prior to the requested access begin date or clearance expiration date. Requests to expedite a clearance will be considered on a case by case basis. Requests for clearances for Central Office may be sent directly to the CCU secured fax or email account (CR, Centralized Clearance) after the authorized Department requestor has completed Section B of the form. Section B must be completed by the requestor or the form will not be processed. The requestor should not retain personal copies of submitted forms; and***

b. ***notifying the CCU when a clearance should be inactivated due to voluntary separation or loss of privileges. (The clearance and any issued Department photo ID must be deactivated.)***

C. Consistent with the Prison Rape Elimination Act (PREA)

1. Prior to the engagement of any contractors, the contractor and all of the contractor's employees and/or subcontractors that may have contact with inmates ***shall*** be investigated to ensure that the Department does not enlist the services of any person(s) who:

a. has engaged in sexual abuse in a prison, jail, lockup, community facility, juvenile facility, or other institution, as defined in 42 U.S.C. §1997 **(28 C.F.R. §115.17 [a][1])**; and/or

b. has been convicted or civilly or administratively adjudicated for engaging or attempting to engage in sexual activity in the community facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse. **(28 C.F.R. §115.17 [a][2] and [3])**

Issued: 4/30/2018
Effective: 5/23/2018

2. The Department shall ***also*** consider any incidents of sexual harassment when determining whether to enlist the services of any contractor who may have contact with inmates. **(28 C.F.R. §115.17 [b][*2*])**

3. If a contractor or the contractor's employee or subcontractor indicates on the **Centralized Clearance Check Information Request Form (Public)** that he/she has worked in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution, as defined in 42.U.S.C. §1997, the requestor shall send a **PREA Current/Prior Employer Letter** to that candidate's previous employer, wait two weeks for a response from the employer, document the request for information, and provide that documentation to the facility Security Office. **(28 C.F.R. §115.17[c][*2*])**

D. Facility Security Office

1. The **Centralized Clearance Check Information Request Form (Public)** shall be forwarded to the facility Security Office for processing in its entirety. Security Office staff shall enter the data into the centralized clearance database and ***process the centralized clearance***. If the candidate's information is already in the centralized clearance database, the appropriate facility Security Office staff member shall make any necessary updates to the database.

2. Any updates to a statewide centralized clearance shall be ***made by the*** facility Security Office staff member.

3. The facility Security Office/CCU shall advise Department staff requestors if a candidate's clearance request has been approved/disapproved, and if warranted, that a specific restriction has been designated. Specific details for disapprovals shall not be furnished to the applicant to avoid illegal dissemination of information. ***All disapproved Centralized Clearance Check Information Request Forms (Public) should be retained for one year. A candidate may not submit a new request until one year has elapsed from the disapproval date***.

4. Only designated facility Security Office staff members, designated Central Office Security staff members, selected staff from the ***Bureau of*** Investigations and Intelligence (***BII***), ***and*** Bureau of Information Technology (BIT) staff shall have authorization to access the complete centralized clearance database, due to the protected and restricted information maintained within this database.

5. All original **Centralized Clearance Check Information Request Forms (Public)** from the field shall be sent directly to the Intelligence Captain/designee for investigation under the centralized clearance procedures. A copy of the completed **Centralized Clearance Check Information Request Form (Public)** may be maintained in the Security Office and/or the CCU for the duration of the clearance period.

6. Consistent with PREA, the facility Security Office shall maintain a copy of the **Centralized Clearance Check Information Request Form**, a copy of the **PREA Current/Prior Employer Letter**, and a copy of the information provided from the

previous employer for ***seven*** years, for all contractors who indicate that they have worked in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution, as defined in 42 U.S.C. §1997. **(28 C.F.R. §115.17[a])**

7. The facility Security Office shall ensure that all affected facility staff are trained on how to handle the notification alerts associated with expired clearances and photos.

8. The Secretary, Deputy Secretaries, Facility Managers, Deputy Superintendents, Majors, Business Managers, Facility Maintenance Managers, Shift Commanders, ***and facility PREA Managers*** shall have access to the web-based listing within the database of approved candidates for specific programs. ***The facility Security Office shall request limited view access for eligible staff members at their respective facilities***.

E. Centralized Clearance Unit (CCU)

The CCU is responsible for the following:

1. processing clearance requests for Central Office access;

2. processing clearance requests for ***Central Office*** projects submitted by the Central Office Bureau's designated liaison;

3. processing clearances for the PA Prison Society, agency temps, ***Vendor II***, contract service providers, and ***rape crisis advocates***; **(28 C.F.R. §115.17[d])**

4. serving as Application Administrator of the centralized clearance system;

5. developing application enhancements and testing the system;

6. developing/conducting training for all system users;

7. managing the security system for the centralized clearance system;

8. assisting the facilities with processing centralized clearance requests;

9. reviewing contested facility-level clearance request disapprovals and making determinations regarding the same;

10. auditing access/entries for completeness, accuracy, and compliance with state, federal, and statutory regulations; and

11. conducting criminal history checks on all contractors every two years. The CCU will contact the applicable facility and requestor and communicate its findings in accordance with Department policy **4.1.1. (28 C.F.R. §115.17[e])**

F. *Processing of Centralized Clearances*

1. ***The facility Security Office/CCU shall complete a full clearance check on all contract service providers, interns, and all medical staff submitted for agency temp positions. A full clearance check includes a query of the following systems:***

    a. ***National Crime Information Center/Commonwealth Law Enforcement Assistance Network (NCIC/CLEAN) criminal history;***

        (1) ***Driver License Query (DQ);***

        (2) ***Pennsylvania Master Name Index (MN) and if applicable, Pennsylvania Rap Sheet (RS); and***

        (3) ***Interstate Identification Index (III) Inquiry (QH) and if applicable, III Rap Sheet Request (QR).***

    b. ***Pennsylvania's Justice Network (JNET) driver's history;***

    c. ***JNET secure web docket sheets;***

    d. ***visitor tracking;***

    e. ***inmate telephone calls (Securus Technologies);***

    f. ***email and monetary transactions (Global Tel Link and JPay); and***

        NOTE: If any flags or warrants are produced from a NCIC/CLEAN criminal history search, the operator should contact that respective criminal justice agency.

    g. ***results of the PREA Current/Prior Employer Letter.***

2. ***The facility Security Office/CCU shall complete a limited clearance check on volunteers, agency temps (non-medical), mentors, reentry service providers, official visitors, public visitors, organizations, Commonwealth Employees (non-DOC), and vendors. A limited clearance check includes a query of the NCIC/CLEAN criminal history system (in accordance with Subsection F.1.a. above) and a review of the results of the PREA Current/Prior Employer Letter, if applicable (28 C.F.R. §115.17[c]).***

3. ***Information obtained during the full or limited clearance check will determine a candidate's approval or denial.***

    a. ***A contract service provider, intern, or medical staff submitted for agency temp positions will be disapproved based on the same criteria for those job***

applicants having prior adverse contacts with criminal justice agencies in accordance with Department policy 4.1.1, Section 41.

b. ***Volunteers, agency temps (non-medical), mentors, reentry service providers, official visitors, public visitors, organizations, and/or vendors will be disapproved for the following:***

(1) ***falsification or omission of pertinent information on the Centralized Clearance Check Information Request Form (Public);***

(2) ***pending misdemeanor or felony criminal charges;***

(3) ***any active warrants (excluding bench warrants);***

(4) ***currently under the supervision of the Pennsylvania Board of Probation and Parole (PBPP), any other probation supervision or currently participating in or awaiting acceptance into an Accelerated Rehabilitative Disposition (ARD), Intermediate Punishment Program (IPP), or other diversion program;***

(5) ***a maximum sentence expiration date from the Department of Corrections (DOC) or release from the supervision of the PBPP within one year with an underlying offense which occurred more than five years ago;***

(6) ***any misdemeanor conviction, in which less than two years has elapsed since the date of conviction and less than one year has elapsed since the release from supervision or confinement;***

(7) ***any felony conviction, in which less than five years has elapsed since the date of conviction and less than one year has elapsed since the release from supervision or confinement;***

(8) ***previous DOC employee, contract service provider, or volunteer whose services were involuntarily terminated; and***

(9) ***current and enforceable protection from abuse orders from staff or inmates.***

c. ***Disclosed communications with an active inmate (visits, telephones calls, emails, mail, or monetary transactions) within three months from the signature on the Centralized Clearance Check Information Request Form (Public) will be disapproved for only that respective facility. This information is to be documented in the centralized clearance system.***

4. ***Any vendor requesting access to DOCInfo should be classified as a Vendor II and an intermediate background check is required. This check will then be documented***

in the centralized clearance system. This includes all the queries outlined in Subsection F.1. above of this procedures manual.

5. ***It is within the discretion of the Facility Manager/designee to permit or deny volunteers, agency temps, mentors, reentry service providers, official visitors, public visitors, organizations, and/or vendors to serve in his/her facility.***

G*. Pennsylvania Prison Society (PPS)*

1. ***The PPS will provide the Centralized Clearance Check Information Request Form (Public) to the CCU to be entered into the centralized clearance system. The CCU will complete a limited clearance check on all PPS members (in accordance with Subsection F.2. above).***

2. ***A visitor tracking query will also be conducted on each PPS member and, if they are active on the personal visitor list, they will not be permitted to visit that respective institution as an official visitor. (See Department policy 1.1.6, "Volunteers and Interns in the Department," Section 6.)***

3. ***A list of the PPS members will be maintained by the CCU and distributed to all facilities on a monthly basis.***

4. ***Names of PPS members who would otherwise be denied clearance, will be provided to the PPS liaison for further discussion with PPS. These members will not be denied by PA DOC, but may be denied by PPS and, subsequently, removed from the approved list.***

CENTRALIZED CLEARANCE CHECK INFORMATION REQUEST

Please type the following information. Enter N/A in any space that does not apply. **All information will be maintained confidentially, but must be provided in order to complete a clearance check.** *Falsification or omission of pertinent information will be considered as justification for disapproval or possible criminal prosecution. It is the responsibility of the requestor to initiate renewal of all clearances. Applicant shall submit this request form to the facility or respective Central Office moderator. Use additional sheets if necessary.*

SECTION "A" (CANDIDATE)

Have you ever worked in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution? ☐ Yes ☐ No

Have you ever been adjudicated, convicted, or otherwise disciplined for committing an act of sexual abuse or sexual harassment in the workplace or community? ☐ Yes ☐ No

Type of Clearance: ☐ Initial Clearance Request ☐ Renewal Request

Category:
☐ Agency Temp Services ☐ Contract Service Provider ☐ Intern/Extern ☐ Organization
☐ Reentry Services ☐ Vendor ☐ Volunteer Program
☐ Official Visitor **(please select one):**
☐ Government ☐ PA Prison Society
☐ Public Visitor **(please select one):**
☐ Ministry ☐ Criminal Justice Agency ☐ Entertainment, Sports, Activities, Guest Speaker
☐ Other **(please explain):**

Purpose of Visit:				Primary Facility:	
Organization/Agency/Company/Program Name:				Abbreviation (if applicable):	
Subcontracted to:			Title or Position:		
Last Name:		First Name:		Middle Name:	
List all previous names:					
Date of Birth:		Social Security Number:			
Passport #:		Alien Registration #:		Visa #:	
Sex:	Race:	Height:	Weight:	Eye Color:	Hair Color:
Current Address:		City:		State:	Zip Code:
Prior Address:		City:		State:	Zip Code:
Place of Birth:		Email Address:			
Home Phone:		Alternate Phone (cell):			
Current Driver's License Information:	State:	Operator: ☐ ID Only license: ☐	OLN Number:	Valid: Yes ☐ No ☐	
Previous Licenses (List all states & #'s that apply):	State:	Operator/Non-Operator #:			
Professional/Medical Licenses:		DEA Number:	NPI Number:		
Identify names, relationships, and locations of any relatives or close friends in any DOC facility:					

I confirm that all information contained on this clearance request has been verified by me to be complete and accurate. I also agree to abide by all Department rules and assume all risks which may result from the normal operation of a Department facility.

Signature:	**Date:**

SECTION "B" (REQUESTING DOC STAFF MEMBER)

Requesting Staff Member:	Employee #:	Date of Request:
Describe Specific Event or Access:	Specific Period of Access Required:	

Section 5 – NCIC/CLEAN/JNET

National Crime Information Center/Commonwealth Law Enforcement Assistance Network/Pennsylvania's Justice Network (NCIC/CLEAN/JNET) systems shall be accessed by trained personnel who require this access for the routine operations of their position. This section is intended to address the requirements for those individuals with access to these systems or who may be granted physical access to areas where such systems may be physically located. Information shall be utilized for official purposes and shall be disseminated to Department staff who have a legitimate need-to-know/right-to-know, and shall not be disseminated to any outside source. The dissemination of information obtained from or through CLEAN to anyone outside the criminal justice or law enforcement community is strictly prohibited.

A. Personnel Requirements

1. Agency employees having access to CLEAN workstations and systems (DOCInfo), as well as the possibility of hearing or viewing Criminal History Record Information (CHRI), shall have a Livescan fingerprint-based background completed as well as a state and national criminal record check run through CLEAN, prior to the individual being allowed access.

2. Unescorted access by support personnel, such as Contract Service Providers, Vendor II, custodial workers, general maintenance contractors, and local government officials, to include those who have direct responsibility to configure and maintain computer systems and networks with direct or virtual access to CLEAN workstations and systems shall have a Livescan fingerprint based background check completed regardless of who employs them, as well as a state and national criminal record check run thorough CLEAN, prior to the individual being allowed access.

3. Authorized personnel are those persons who have passed a fingerprint-based record check and a state and national criminal record check through CLEAN.

4. A two-year recertification is required on all above personnel. (State and National criminal record check through CLEAN) **(PSP: Admin Regs, Ver. 6 [K] 4 or current version)**

B. Security Awareness Training Requirements

All personnel/contractors/vendors who have unescorted access must complete Security Awareness training every two years through Criminal Justice Information System (CJIS) On-Line (www.cjisonline.com), except for CLEAN certified operators. Certified operators will receive their Security Awareness training every two years during recertification testing. All unescorted personnel shall be provided the Security Awareness training within six months of initial assignment. All Information Technology (IT) personnel who obtain Level 4 Security Access must fill out a CJIS Security Addendum. **(PSP: Admin Regs, Ver. 6 [J] 1 or current version) (CJIS Security Policy: Ver 5.6 [Security Awareness Training] 5.2)**

Issued: 2/6/2023
Effective: 2/13/2023

C. Security

1. The data stored in and available through the NCIC/CLEAN/JNET systems or related electronic informational databases, is documented Criminal Justice Information (CJI) and must be protected to ensure correct, legal, and efficient dissemination and use. The systems must be secure from any unauthorized use. Non-public criminal history information or restricted information obtained through these systems may not be transmitted through non-encrypted electronic transfer. Only those Department personnel who have met all state/federal requirements shall have indirect access to restricted information obtained directly from these systems.

2. The data stored and available through NCIC/CLEAN/JNET is CONFIDENTIAL and must be treated accordingly. Any unauthorized request or receipt of restricted material could result in administrative, civil, or criminal proceedings.

D. Individual Direct Access to NCIC/CLEAN/JNET

1. Access is restricted to criminal justice employees who have no significant conviction records. Any individual will permanently lose direct CLEAN or CJIS access for a conviction of any of the following:

   a. any felony;

   b. any misdemeanor for which more than one year in prison can be imposed as punishment; and

   c. any computer crime.

2. Criminal justice officials with direct access to CLEAN or CJIS arrested or indicted for any of the following will lose access to CLEAN or CJIS until disposition of charges:

   a. any felony;

   b. any misdemeanor for which more than one year in prison can be imposed as punishment;

   c. any computer crime; and

   d. any misdemeanors where there are two or more counts from separate criminal complaints/incidents.

E. Testing and Certification

1. Initial training and certification must be completed within 90 days from the start of the certification process. Refer to **JNET Access Request Process for New Users Form (Attachment 5-A**) and **JNET Auto Registration Quick Reference for New CLEAN Users (DOC and Parole) (Attachment 5-B)**.

Issued: 2/6/2023
Effective: 2/13/2023

2. Biennial recertification tests must be completed prior to expiration date.

F. Dissemination

1. NCIC/CLEAN information may be disseminated to another authorized Criminal Justice Agency (CJA) in conjunction with an official purpose only. Release of any CLEAN/NCIC information to another CJA must be logged as a secondary dissemination. All secondary dissemination of CHRI obtained from NCIC/CLEAN or Pennsylvania Department of Transportation (PennDOT) records must be logged on the **CHRI Dissemination Log (Attachment 5-C)** and the log must be kept for a minimum of three years for CHRI and five years for PennDOT data.

2. Criminal history extracted from these systems may never be disseminated to any Non-Criminal Justice Agency (NCJA) or individual.

3. All CHRI information extracted from the system must be destroyed after its intended use has expired. At no time shall CHRI information be stored, copied, filed, saved on computers, scanned into case management systems, etc. Acceptable methods of destroying data obtained from NCIC/CLEAN is shredding, burning, or elimination of identifying information.

G. CLEAN/JNET Field Coordinator

1. Each facility or field office shall designate a CLEAN/JNET Field Coordinator as the liaison to the Terminal Agency Coordinator/JNET Terminal Agency Coordinator (TAC/JTAC) for NCIC/CLEAN/JNET operations. A Field Co-Coordinator is also suggested. These individuals must have at a minimum one-year experience as a certified CLEAN and JNET operator who will be responsible for the CLEAN/JNET operators at their respective institutions.

2. Coordinators and Co-Coordinators shall be nominated by the Deputy Superintendents or Parole District Director/designee and submitted to the TAC/JTAC for approval of assignment.

3. Each facility shall maintain a sufficient number of certified operators to ensure 24-hour coverage for the Control area, as well as normal operational routine of the facility.

H. Responsibilities of Field JNET/CLEAN Coordinators

1. Maintain a resource email account for all CLEAN/JNET users at their Institutions.

2. Point of contact for CLEAN/JNET users at their facility for questions, training, trouble shooting, resetting passwords, etc.

3. Coordinator will ensure that all CLEAN users are completing their recertification test (every two years) prior to their accounts expiring.

4. Coordinators will ensure that all personnel are completing the Pennsylvania State Police (PSP) Security Awareness Training every two years in CJIS Online. Coordinator will inform the TAC of any CLEAN/JNET user that is no longer employed, transferred, or no longer requires access to CLEAN/JNET for removal or transfer of accounts.

I. Physical Security

1. The computer site and/or device area must have adequate physical security to protect against unauthorized personnel gaining access to the computer equipment (CLEAN terminal, Livescan).

2. All changes concerning the equipment connected to NCIC/CLEAN must be coordinated through the TAC/JTAC to include relocation of equipment, upgrading existing equipment, and acquiring additional equipment.

3. All State Correctional Institutions (SCIs) must have a stand-alone CLEAN terminal located in Control, Security, and Records departments. All personnel within these areas are required to be CLEAN Certified. All stand-alone CLEAN terminals must be logged into every day.

4. NCJA who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Department of Corrections and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

5. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the Department of Corrections and each private contractor personnel. Each private contractor personnel will appropriately have a state and national fingerprint-based record background check prior to this restricted area access being granted.

6. All personnel with CJI physical and logical access must:

    a. meet the minimum personnel screening requirements prior to CJI access:

        (1) to verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI;

        (2) support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel always; and

(3) prior to granting access to CJI, the Department of Corrections on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

b. complete security awareness training:

all authorized Department of Corrections, NCJA, and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.

J. Expungement

Upon receipt of official notification of expungement, the Department shall remove any evidence of said criminal history from Department documents. This expungement order shall be forwarded to all agents who were recipients of this disseminated information. Once the information is expunged, the expungement order shall be destroyed.

K. Audits

1. PSP shall triennially audit each facility or Parole Field Office with access to CLEAN information. The audit shall be conducted to ensure compliance with CLEAN/CJIS regulations, as well as federal and state statutes on security and privacy of CHRI.

2. Questions relating to the operation of NCIC/CLEAN/JNET, policy modifications, or dissemination of this computerized information shall be directed to the Central Office TAC/JTAC.

L. Disciplinary

1. In support of the Department of Corrections mission of public service to the citizens of Pennsylvania, the Department of Corrections provides the needed technological resources to personnel to access Federal Bureau of Investigation (FBI) CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI CJI or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care, and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, mobile devices, live scan devices, fingerprint scanners, software, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by the Department of Corrections, state CJIS Security Officer (CSO), and the FBI. To maintain the integrity and security of the Department of Corrections and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations, and contractual obligations. All existing laws and Department of Corrections regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

2. Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of the Department of Corrections computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

   Examples of misuse with access to FBI CJI.

   a. Using someone else's login that you are not the owner.

   b. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access Department of Corrections systems and/or FBI CJIS systems and data in your name.

   c. Allowing unauthorized person to access FBI CJI at any time for any reason.

      NOTE: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.

   d. Allowing remote access of Department of Corrections issued computer equipment to FBI CJIS systems and/or data without prior authorization by the Department of Corrections.

   e. Obtaining a computer account that you are not authorized to use.

   f. Obtaining a password for a computer account of another account owner.

   g. Using the Department of Corrections network to gain unauthorized access to FBI CJIS.

   h. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.

   i. Knowingly propagating a computer virus, Trojan horse, worm, and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.

   j. Violating terms of software and/or operating system licensing agreements or copyright laws.

k. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in the Department of Corrections, for home use or for any customer or contractor.

l. Deliberately wasting computing resources to include streaming audio or videos for personal use that interferes with Department of Corrections network performance.

m. Using electronic mail or instant messaging to harass others.

n. Masking the identity of an account or machine.

o. Posting materials publicly that violate existing laws or Department of Corrections codes of conduct.

p. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.

q. Using Department of Corrections technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.

r. Unauthorized possession of, loss of, or damage to Department of Corrections technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

s. Maintaining FBI CJI or duplicate copies of official Department of Corrections files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

t. Using the Department of Corrections technology resources and/or FBI CJIS systems for personal or financial gain.

u. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

v. Using personally owned devices on Department of Corrections network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store Department of Corrections data, State data, or FBI CJI.

3. The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by the Department of Corrections on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate Department of Corrections officials for security or performance testing.

M. Privacy Policy

All agency personnel utilizing agency-issued technology resources funded by the Department of Corrections expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Department of Corrections systems indicates consent to monitoring and recording. The Department of Corrections reserves the right to access and audit all communications including electronic and physical media at rest, in transit, and at end of life. Department of Corrections personnel shall not store personal information with an expectation of personal privacy that are under the control and management of the Department of Corrections.

N. Disposal of Media

1. When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store, and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by the Department of Corrections.

2. Acceptable methods of destroying data obtained from NCIC/CLEAN is shredding, burning, or elimination of identifying information.

3. Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier, hard drives, etc.) shall be disposed of in accordance with measures established by the Department of Corrections.

4. IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from the Department of Corrections control until the equipment has been sanitized and all stored information has been cleared.

O. User Account/Access Validation

1. All accounts shall be reviewed at least every six months by the TAC or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain CJI. The TAC may also conduct periodic reviews.

2. All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

3. 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) should be disabled.

4. 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.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

5. The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

6. Primary responsibility for account management belongs to the TAC.

   The TAC shall:

   a. modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.;

   b. periodically review existing accounts for validity (at least once every six months); and

   c. cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

P. Warrants

1. Per **PSP CLEAN TAC Manual Appendix G** there needs to be Record Accountability, Accuracy, Timeliness, and Quality Control for all warrants entered.

2. Agencies that have records in NCIC are responsible for the accuracy, timeliness, and completeness.

3. The accuracy of the record must be double checked by a second party within 72 hours of the warrant being entered.

4. Verification should require the case officer to check the accuracy of the record, as the case officer carries the primary responsibility for seeking the fugitive or stolen property.

5. The final responsibility of the accuracy of the record is the agency whose originating agency identifier (ORI) appears on the record.

6. CLEAN/NCIC records must be entered promptly to ensure maximum system effectiveness.

7. Timely modification of a CLEAN/NCIC record means as soon as possible following the detection of the erroneous data in an existing record or as soon as possible following the receipt of data not already stored in the record.

8. All entries into CLEAN/NCIC must be checked by a 2nd party for accuracy.

Agency Temp – Temporary staff hired through medical staffing agencies covering Physicians, Physicians Assistants, Psychiatrists, Dentists, Nurses, and CRNPs. They are to be processed and validated by the Bureau of Health Care Services. All other temporary staff shall be characterized under the "Vendor" category.

Centralized Clearance – Process by which a Department employee requests clearance approval on behalf of a non-Department staff member, prior to institution activity related events. Non-Departmental staff shall be required to submit a new clearance request form on a biennial basis (every two years). The designated form with processing instructions is available on the Department's public website at www.cor.pa.gov. Candidates shall indicate their level of clearance request, justification, and disclosure of all personal descriptors to facilitate this process. Candidate will then submit this form to their Department requesting staff member for validation and submission to the facility Security Office or the Centralized Clearance Unit (CCU).

Centralized Clearance System – An application within DOCNet which includes the vital statistics of the candidate requesting access to Department institutions/information, as well as the approving authority's related information. The system shall be administered by the Centralized Clearance Unit (CCU) and direct access to this system is restricted to authorized Department Central Office Security staff, ***Bureau of*** Investigations and Intelligence (***BII***), facility Security Office staff, and associated Bureau of Information Technology (BIT) staff. Dissemination of this information is restricted to authorized Criminal Justice Agency staff only. Completed hard copies of the **Centralized Clearance Information Request Form** or restricted information obtained from this form may only be retained within the institution Security Office/CCU. Limited access to this system will be provided to designated Departmental staff by the CCU Administrator indicating type of access, level of access, organization, and clearance dates of all clearance candidates.

Centralized Clearance Unit (CCU) – The CCU is the Department assigned unit within Central Office which is responsible for the complete administration of the centralized clearance process. The unit shall be responsible for providing all training, maintaining the restricted database, security administration, system enhancements, conducting designated sensitive or confidential clearances and shall arbitrate all candidate appeals or institution variances. This unit shall ***process*** clearances for Contract Service Providers, PA Prison Society Official Visitors, agency temporary staff, ***rape crisis advocates, and Vendor II from Central Office requestors***. This unit will also conduct queries of candidates requesting Central Office access or whose requesting staff member is assigned to Central Office. ***All requests will be processed as*** Statewide clearances.

Certified CLEAN Operator – An employee who has completed official training, passed testing requirements, is currently in active status, and certified by the Department's System Agency Coordinator and the Pennsylvania State Police (PSP). Operators will be fingerprinted, sign statements of liability, and supplemental backgrounds will be conducted on these candidates as required by the PSP prior to the issuance or renewal of this certification.

Contract Service Provider (CSP) – A business or individual that provides goods or services to the Department for monetary reimbursement which includes the care, custody, and control of inmates. (For example: staff directly employed by a primary contractor covering medical, mental

health (agency temp), treatment or contract chaplains.) Part-time staff within these categories may also be characterized as CSPs, however, must submit to the CSP process and all required training. (Any part-time CSP that does not complete this process or any subcontractor to the CSP Agency must be supervised by Department staff at all times and shall be considered a vendor.) Clearances for CSPs may be approved for a period of up to 24 months.

Criminal Justice Agency – Any court, including the minor judiciary, with criminal jurisdiction or any other governmental agency, or subunit thereof, created by statute or by the State or Federal constitutions, specifically authorized to perform as its principal function the administration of criminal justice, and that allocates a substantial portion of its annual budget to such function. Criminal justice agencies include, but are not limited to, organized state and municipal police departments, local detention facilities, county, regional and state correctional institutions, probation agencies, district or prosecuting attorneys, parole boards, pardons boards, and such agencies or subunits thereof, as declared by the Office of Attorney General to be criminal justice agencies as determined by a review of applicable statutes and the State and Federal constitutions, or both.

Criminal History Information – Information collected by criminal justice agencies concerning an individual 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 from those charges. All criminal history obtained from NCIC/CLEAN/NLETS/JNET shall be maintained according to the Criminal History Record Information Act (Title 18, Chapter 91).

Department – The Pennsylvania Department of Corrections.

Disclaimer Stamp – A stamp provided to each Department NCIC/CLEAN/JNET terminal site specifying the following:

"This document is an original copy and should not be reproduced without following the criteria established in CHRIA. All reproduced copies of this document should be logged before dissemination. This CHRI is only that which is contained within Department files. A summary of statewide CHRI may be obtained from the Pennsylvania State Police, Records and Identification Division."

Dissemination Log – The written log retained at the access terminal site that contains the name inquiry, date of birth, social security number, the date of request, the title and name of the person making the request for this information, initials of the operator, reason for the request, purpose code, and recipient of information.

Dissemination/Destruction Sheet – Documentation of transfer of NCIC/CLEAN/JNET criminal history information to a third party within the Department or to an outside criminal justice agency when applicable. Documentation shall include chronological entries of subject's name and title of the individual requesting the information, and the purpose of the request for this information. Dissemination sheets shall also include destruction related information.

Expungement – The removal of any indication of criminal information maintained within Department files so that there is no trace or indication that such information existed. Expungement orders shall be forwarded to all individuals that have received the original information to be expunged. All copies of the order shall be destroyed when expungement has been completed.

Full Access – Access given to contract service providers, interns, and all medical staff submitted for agency temp positions. Following the security orientation, these individuals do not require supervision or an escort throughout the facility.

Full Clearance Check – Includes a query of the NCIC/CLEAN criminal history, Pennsylvania's Justice Network (JNET) driver's history, JNET secure web docket sheets, visitor tracking, inmate telephone calls, inmate emails, monetary transactions, and results of the PREA Current/Prior Employer Letter.

Inmate Visitor – Any individual who, under supervision of security staff, engages in an approved inmate visit using the facility visiting room or assigned visiting area. Inmate must submit appropriate request documentation for approval to include the visitor's name, DOB, address, and relationship. Attorney rooms may be requested if the interview requires confidential access.

JNET – Pennsylvania's Justice Network (JNET) is the Commonwealth's integrated justice portal, which provides a common online environment for authorized users to access shared public safety and criminal justice information for official purposes only.

JNET Criminal History User – This role, when issued to a JNET Criminal Justice User, provides them with the elevated access to the Pennsylvania State Police (PSP), Computerized Criminal History Record Information (CCHRI) and the National Crime Information Center (NCIC). If the position warrants, this user status may also allow access to other agency secured sites provided all supplemental training has been completed. Users requesting access to this role must be PSP CLEAN certified under the direction of the Department System Agency Coordinator.

JNET Criminal Justice User – Users requesting this level of access must be directly employed by a criminal justice agency, need access to this information to carry out his/her official work related duties/functions, and be trained and certified through his/her agency. This role provides Department users with the basic access to JNET which includes public criminal history information and if the position warrants, PennDOT photos.

JNET Registrar – Responsible for the registration and training of all users, maintains agreements, schedules certification installations, initiates key recovery, and manages JNET user provisioning information.

JNET Sponsor – The role of the sponsor is to validate the official need of those individuals applying for access to JNET. The sponsor should have working knowledge of JNET and the responsibilities of those applying for JNET access. Recommended JNET users include those

regularly assigned to cover the following areas of responsibility: Inmate Records, Human Resources, and Commissioned Officers assigned to Control or the facility Security Office.

JNET Terminal Agency Coordinator (JTAC) – The JTAC is the Department's point of contact relating to the access of elevated applications within JNET that contain criminal history information. The JTAC is the liaison between the Department and JNET, PSP, and the FBI/CJIS. As the administrator, this position is also responsible for enforcement of all state/federal regulations relative to all criminal justice systems including the certification process of users authorized for the upgrade to Criminal History User status. Extensive experience in both PSP CLEAN Portal XL and JNET CLEAN is required to maintain this position. Basic information technology knowledge is preferred.

Limited Access – Access given to volunteers, agency temps (non-medical), mentors, reentry service providers, official visitors, public visitors, organizations, Commonwealth Employees (non-DOC), and vendors. These individuals shall be supervised and escorted by Department staff at all times while in a Department facility or when outside the secure perimeter.

Limited Clearance Check – Includes a query of the NCIC/CLEAN criminal history system and review of the results of the PREA Current/Prior Employer Letter (28 C.F.R. §115.17[c]), if applicable, for those individuals receiving limited access.

Mentor – An approved private citizen, organization, or government entity designated by the Department to provide developmental support to inmates accepted into the Department's Reentry Program. Visitation for mentors that are private citizens will be restricted to the Inmate Visiting Room. Visitation for approved organizations or government entities may be conducted in designated areas within the Transitional Housing Unit.

NCIC/CLEAN/JNET Field Coordinator (FC) – The NCIC/CLEAN Field Coordinator or the JNET Field Coordinator is a Department certified operator designated by the Superintendent as the liaison between the System Agency Coordinator and his/her respective facility. The FC is responsible for ensuring compliance with Federal and State guidelines at his/her respective institutions; developing local procedures, ensuring the security and maintenance of the equipment, conducting in-service training, and re-certification testing of institution operators.

NCIC/CLEAN/NLETS – NCIC is an acronym, which stands for the "National Crime Information Center." CLEAN standards for the "Commonwealth Law Enforcement Assistance Network." NLETS standards for the "National Law Enforcement Telecommunications System." Together they establish a computerized information system as a service to all criminal justice agencies – local, county, state, and federal, by providing and maintaining a computerized filing system of accurate and timely criminal justice information.[1] Information relating to operator licensing and vehicle registration records is made available through a CLEAN computer-to-computer interface with the Department of Transportation and through NLETS. Access to this system also avails the Department to a telecommunications system and specific automated functions such as: the Interstate Identification Index, PA automated rap sheets, road/weather information, hazardous

[1] 5-1F-4102 (5-ACI-1F-08)

materials, wanted persons, agency directories, and any other function as designated by the Pennsylvania State Police Control Terminal Agency. Information extracted from this system is to be used for official purposes only.

Official Visitor (Government) – The Governor, Lieutenant Governor, President pro tempore and members of the Senate, Speaker and members of the House of Representatives, justices and judges of the courts of record, the General Counsel, the Attorney General and his/her Deputies as part of their official duties are not required to submit any documentation to the Centralized Clearance Unit (CCU), ***Bureau of*** Investigations and Intelligence (***BII***) prior to their visiting a Department institution, provided they continue to serve in their official governmental capacities. One employee of the above noted officials may also accompany the government Official Visitor when visiting any correctional institution and may be present during an interview.

Official Visitor (Pennsylvania Prison Society) – Members of the PA Prison Society who have been designated as official visitors, shall submit their centralized clearance request forms directly to the Centralized Clearance Unit (CCU). Members whose terms have expired will be suspended until a ***renewal centralized clearance is submitted and processed***. Clearances may be approved for a maximum of two years, but should expire at the termination of their active membership is less than two years. Visitation shall take place in the Inmate Visiting Room or specific designated area within the institution. Attorney rooms may be requested if the interview requires confidential access.

Originating Agency Identifier (ORI) – The Originating Agency Identifier (ORI) is a nine character, alphanumeric identifier assigned by NCIC to every agency that is qualified to have access to information stored in the NCIC computer. All ORIs shall begin with the assigned state abbreviation.

Public Visitor (Non-Inmate Visitor) – Any person from the community who requests access into an institution on behalf of the Department for meetings, special projects, worship services, or similar events. These persons usually include, but are not limited to, sporting teams, outside entertainment, athletic officials, church choirs, organizations, religious affiliates, or other federal/state/county agencies, etc. These individuals have limited or no direct inmate contact. Department staff supervises his/her meetings at all times. The individual sub-categories of Public Visitors are categorized as: Public Visitor (Ministry), Public Visitor (Criminal Justice Agency), Public Visitor (Entertainment, Sports, Presentations, Activities), and Public Visitor (Government Agency).

Rap Sheet – Rap sheet stands for “Record of Arrest and Prosecution” and it a history of an individual’s criminal report.

Reentry Services – Federal, state, county, local, and community groups/agencies dedicated to the effort to have optimum resources available for the reintegration of inmates prior to and upon their release from prison.

Requestor – An authorized Department staff member who is requesting the candidate’s clearance request. Non-Department staff may not act as requestors.

System Agency Coordinator (SAC)/JNET Agency Coordinator (JSAC) – The System Agency Coordinator (SAC) and the JNET Agency Coordinator (JSAC) are the individuals within the ***Bureau of*** Investigations and Intelligence (***BII***) designated by the agency head, who are responsible for ensuring compliance with CLEAN/NCIC/NLETS/JNET policies and regulations. An institution liaison shall be designated as the field coordinator for JNET/CLEAN. These individuals act as the official liaison between his/her agency, PSP, FBI, and JNET. The duties of the SAC/JSAC include, but are not limited to, quality control assurance, internal audits, certification training of new operators, updated training, indirect supervision of CLEAN or JNET field coordinators, functional testing, problem solving, and misuse investigations.

Vendor – Business or individual that provides goods or services to the Department for monetary reimbursement. Vendors that are issued a centralized clearance must be escorted by Department staff at all times and have very limited or no inmate contact. Vendors that have had any centralized clearance (such as common carriers for deliveries or emergency delivery of supplies), must remain under escort by security staff whenever within the secured perimeter of the institution or any Department staff if outside the secure perimeter. Vendors (Level 1) shall submit to a clearance check initially and ***biannual renewal requests as appropriate.*** Vendors (Level 2) status are those that have an elevated access to unrestricted inmate information, confidential documents, internal policies or any information that is covered by the CHRIA act. These individuals shall receive a ***full*** level clearance check as characterized by the Centralized Clearance Unit and shall be required to submit fingerprints to be classified by PSP and the FBI. System queries for level 2 vendors shall utilize the purpose code of “J.”

Volunteer – A person from the community, who has direct contact with an inmate, and on a regular basis without compensation, offers services, programs, education, or other assistance to an inmate. Volunteers must complete the expanded application process and all required training. An individual who volunteers his/her services on an occasional basis without compensation may be included as a Volunteer, however, if characterized in this manner, submit to the expanded application process and all required training. (Any individual who occasionally volunteers his/her time but does not complete this process must be supervised by Department staff at all times and shall be considered a Public Visitor). Clearances may be approved for Volunteers up to a period of two years.