CLEVELAND DIVISION OF POLICE
GENERAL POLICE ORDER

EFFECTIVE DATE:	CHAPTER:	PAGE:	NUMBER:
AUGUST 5, 2022	7 - Communications	1 of 12	7.02.04

SUBJECT:

LEADS/NCIC/INTERFACE INFORMATION SYSTEMS

CHIEF:

Dornat A. Drummond, Chief

PURPOSE: To establish rules and procedures regarding the proper use of the Law Enforcement Automated Data System/National Crime Information Center (LEADS/NCIC) system, Interface Information Systems, Law Enforcement Record Management System (LERMS) and Field Based Reporting (FBR) used by the Division of Police. Improper use of the system or improper distribution of information obtained from the system could result in criminal, civil, and/or Division sanctions.

POLICY: **It is the policy of the Cleveland Division of Police** to utilize the LEADS/NCIC system as an integral and indispensable tool for accessing necessary information for criminal justice purposes; all employees of the Division shall have knowledge of the procedures associated with the use of the LEADS/NCIC operating system, interface information systems and adhere to all guidelines set forth in this order as well as the LEADS/NCIC rules and regulations set forth in the Ohio Administrative Code Chapter 4501:2-10.

DEFINITIONS:

Computerized Criminal History (CCH) - an Ohio electronic data processing file which is accessible using specific data fields. It is a central repository for arrest, conviction, and disposition data on adults and juveniles arrested for felony and gross misdemeanor offenses. The Bureau of Criminal Investigation (BCI) is responsible for storing these records.

Criminal Justice Agency (CJA) - the courts and a government agency, nongovernmental agency, or any sub-unit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part (more than fifty percent) of its annual budget to the administration of justice. Examples include prosecutor agencies, courts at all levels with criminal jurisdiction, corrections departments, probation departments, and parole departments.

Criminal Justice Agency (CJA) User Agreement (**Security Dissemination Form**) **-** a terms of service agreement that must be signed prior to accessing Criminal Justice Information (CJI). This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, etc.

Criminal Justice Information (CJI) **-** the abstract term used to refer to all of the Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS). It provides data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property [when accompanied by any personally identifiable information (PII)], and case/incident history data. In addition, CJI refers to the FBI CJIS provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following types of data are exempt from the protection levels required for

CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information (CJI) Interface Systems - systems used by the Division to obtain CJI using LEADS/NCIC requests and to access previously collected CJI (e.g., incident reports, arrestee information, etc.). This information includes LERMS and FBR.

Criminal Justice Information Systems Officer (CSO) - the individual located within the CJIS Agency responsible for the administration of the CJIS network on behalf of the CJIS Agency.

Digital Media - any form of electronic media designed to store data in a digital format including, but not limited to, memory devices in laptops, computers, and mobile devices as well as any removable, transportable electronic media, such as a magnetic tape or disk, optical disk, flash drive, external hard drive, or digital memory card.

Escort - authorized personnel who accompany a visitor at all times while in a physically secure location to ensure the protection and integrity of the secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Information Exchange Agreement - an agreement codifying the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty of care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards, and guidance.

Law Enforcement Agency - includes all local, county, state, and federal police agencies that are responsible for the enforcement of criminal law.

Law Enforcement Automated Data System (LEADS) - the statewide computerized network which provides computerized data and communications for criminal justice agencies within the State of Ohio. LEADS is administered by the Ohio State Highway Patrol's Superintendent and serves as the electronic communication network for Ohio's criminal justice communities and the gateway to NCIC.

LEADS Fully Qualified Operator (FQO) - any person, typically a Senior Data Conversion Operator (SDCO), who can operate a LEADS access device with the capabilities to enter, cancel, clear, modify, query, locate, detain and submit hit confirmations. Fully Qualified Operators have access to enter information into the LEADS/NCIC system to include wanted persons, missing persons, stolen autos, etc.

LEADS Inquiring Operator (INQ) - any person, typically patrol officers and dispatchers, certified to access a LEADS workstation terminal, mobile data terminal, LERMS or FBR. LEADS Inquiring Operators do not have access to enter information into the LEADS/NCIC system or to access CCH reports.

LEADS Inquiring Operator with CCH (INQ w/CCH) - any person, typically detectives or investigators, certified to access a LEADS workstation terminal, mobile data terminal, LERMS or FBR. LEADS Inquiring Operators with CCH do not have access to enter information into the LEADS/NCIC system but can access CCH reports.

LEADS Practitioner - any person, typically administrative positions, instructors, clerks, securities, traffic controllers, and other agencies who access LERMS, authorized to receive LEADS/NCIC information who is not a certified operator. LEADS practitioners have access to LEADS/NCIC information however they cannot operate the LEADS terminal. This status allows unescorted access within Cleveland Division of Police facilities.

Local Agency Security Officer (LASO) - the primary Information Security contact between a local law enforcement agency and the CJIS agency (CSA) which interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation, including system configuration data, assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Logical Access - the technical means (e.g., to read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system (i.e., LERMS and FBR) to utilize CJI or CJIS applications.

National Crime Information Center (NCIC) - the nationwide computerized filing system established for criminal justice agencies at the local, state and federal levels, which is managed by the FBI. It is a computerized index of open warrants, arrests, stolen property, missing persons, and dispositions regarding felonies and serious misdemeanors.

Physical Access - the physical ability, right or privilege to view, modify, or make use of CJI by means of physical presence within the proximity of computers and network devices (e.g., the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media - refers to media in printed form, including, but not limited to printed documents, printed imagery, or printed facsimile.

Physically Secure Location - a facility or an area, a room, or a group of rooms within a facility with both physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control, state identification bureau control, FBI CJIS Division security addendum, or a combination thereof.

Terminal Agency Coordinator (TAC) - the designated person that serves as the point of contact at a local agency for matters relating to LEADS information access. A TAC administers LEADS systems programs within the local agency and oversees the agency's compliance with LEADS/NCIC system policies. Each agency with LEADS/NCIC access shall appoint a TAC.

Visitor - a person who is a temporary guest at a Division facility, who is not employed by the Division, and has no unescorted access to the physically secure location within the Division where CJI and associated information systems are located.

PROCEDURES:

I. Authorization and Access

A. Individuals who require unescorted access to unencrypted CJI shall be screened.

1. Record checks to verify identification, state of residency or Ohio Bureau of Criminal Identification and Investigation (BCI&I) web check fingerprinting, and national fingerprint based record checks shall be conducted prior to granting access for all personnel including:

a. Division members.

b. Other City employees and vendors who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas within Division facilities.

2. Record checks shall be completed prior to unescorted access to the Division's facilities and before any access into LEADS information systems, including LERMS and FBR.

B. Denial of CJI access.

1. Persons with an existing record of any kind, shall not be granted access to CJI until:

a. The Division makes a determination if access should be granted based upon the type of record or arrest.

b. If the Division determines that access should be granted, a LEADS access review form shall be submitted outlining the explanation.

c. The CSO or designee shall review the matter to determine if access is appropriate.

2. Persons with felony convictions, shall be denied access to CJI; however, the Division may ask for a review by the CSO or designee in extenuating circumstances where the severity of the offense and the time passed would support a possible variance.

3. Persons with a record of misdemeanor offense(s) may be granted access by the CSO or designee.

a. The nature or severity of the misdemeanor offense(s) shall be reviewed to determine if qualification is or is not necessary.

b. The Division may request the CSO review a denial of access determination.

c. The same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

C. CJI access followed by arrest and/or criminal charge.

1. Continued access to CJI shall be determined by the CSO.
   a. This determination is not implicitly granting hiring/firing authority with the CSA, only the authority to grant access to CJI.

   b. For offenses other than felonies, the CSO has the latitude to delegate continued access.

   c. If the CSO or designee determines that access to CJI by the person would not be in the public interest, access shall be denied; the person's appointing authority shall be notified in writing of the access denial, and the person will be placed onto the LEADSDENY list.

2. The Division may appeal the decision made for continued access to CJI determined by the CSO by submitting a letter from the agency administrator outlining the following items:

   a. The applicant's name, date of birth and OLN.

   b. An explanation as to why an appeal should be granted.

   c. The statement, "This agency has internal policies governing the use of LEADS and CJIS access and the employee will be held accountable to these policies and all LEADS administrative rules. I, as the agency administrator, accept ultimate responsibility for this employee's actions in the use of LEADS."

D. The Division shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

II. Account Management and Validation

A. An account can be created by completing the following:

1. CCH records background check performed by LEADS Unit.

2. Fingerprint processing.

3. Successful LEADS training and testing.

4. LEADS/NCIC/OHLEG/LERMS Security Dissemination Form completed and forwarded to the LEADS Unit.

5. Access to LEADS/NCIC through LERMS/FBR will then be granted by the Technology Integration Unit (TIU).

B. The LEADS Unit shall establish, activate, modify, transfer, disable and remove member accounts using the LEADS web portal based on the member's current status and official duties.

C. The TIU shall establish, activate, modify, review, disable and remove a member's accounts using LERMS and FBR interface systems based on the member's current status and official duties.

D. The Public Safety Information Technology (IT) Department shall establish, activate, modify, review, disable and remove a member's accounts using the CAD system based on the member's current status and official duties.

E. The LEADS Unit and the TIU shall identify authorized users of the information system and specify access rights/privileges based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.

2. Satisfaction of all security criteria.

F. The Division shall maintain current Information Exchange Agreements with agencies that use the Division's LERMS information system.

G. The Personnel Unit shall notify the Officer-in-Charge (OIC) of the LEADS Unit and the TIU via email a current departures list for both sworn and non-sworn members of the Division; the LEADS Unit and the TIU shall:

1. Make the appropriate modifications to the member's status in the respective system.

2. Validate information system accounts at least twice a year using the departures list from the Personnel Unit; these validations shall be documented.

III. Mandatory Testing and Training

A. ALL Division members, City employees, and vendors who work inside a physically secure location, or with the information system/network, shall be a LEADS Operator (INQ, INQ w/CCH, FQO w/CCH) or a LEADS Practitioner.

1. Based on certification type, successfully complete CJIS training and testing.

a. Members shall <u>not</u> use previous LEADS tests or other materials to assist them during recertification other than the CJIS manuals provided online, in digital or printed form, including the NCIC Operating Manual, NCIC Code Manual, NCIC Technical and Operational Updates, Interstate Identification Index/National Fingerprint File Manual, LEADS Manual, LEADS Administrative Rules, LEADS Security Policy, International

Justice and Public Safety Information Sharing Network (NLETS) Wiki, Validation Procedures Manual, and the BCI Manual.

b. Per the Exam Retrieval section of the LEADS Manual, "When an operator is ready to test, the agency TAC shall instruct them on how to retrieve the exam. Operators are permitted to use all resources available on the CJIS Launchpad and the LEADS public web site (www.leads.ohio.gov). The TAC is permitted to assist the operator with researching the resources; however, they **CANNOT** give the operators the answers nor are TACs permitted to take the test for them."

2. Complete a LEADS Security Dissemination Form and forward to the LEADS Unit via email at LEADS@clevelandohio.gov.

B. Operators shall:

1. Read the spring and fall issues of the LEADing News publication.

2. Complete the TAC continuing professional training yearly.

3. Sworn members shall complete the Learning Management System (LMS) assignment within two weeks of the assignment date.

C. The LEADS Unit shall:

1. Notify all members and vendors before their certification expires.

2. Include instruction on how to take the LEADS test and forward the completed Dissemination Security Form.

3. Disable the accounts of expired members and vendors.

D. Members shall be responsible for maintaining their certification.

IV. LEADSDENY

A. LEADS and OHLEG administration, along with the OIC of the LEADS Unit and the TIU, shall be notified by the Internal Affairs Unit when a member is arrested or charged with any crime.

1. LEADS will review the evidence of the incident and determine if the member will be placed into LEADSDENY status.

2. Members arrested for or charged with any felony or "serious misdemeanor", as defined in the LEADS Administrate Rules, shall immediately be placed into LEADSDENY status.

3. The LEADS Unit shall modify the member's status in the LEADS system, TIU will make the member inactive in LERMS and FBR.

B. When a member is in LEADSDENY status all access to CJI is denied.

1. This access includes, but is not limited to, direct access, printouts and verbal information obtained from LEADS/NCIC.

2. Any areas where information obtained from LEADS/NCIC may be seen, viewed, or heard (i.e., police radio broadcasts) are not accessible to members in LEADSDENY status.

C. The LEADS Unit shall maintain a current list of Division members, City employees, and vendors on the LEADSDENY list.

D. Appeal/Review.

1. Once all criminal and admistrative proceedings are complete, the member has thirty days to attempt removal from the LEADSDENY list.

2. Denial may only be appealed by a criminal justice agency administrator (i.e., the Chief of Police) under Section 5.12 of the LEADS Security Policy; submitting an appeal does not guarantee it will be granted by the CSO.

3. The incident can be reviewed once the case is adjudicated; LEADS will again review all evidence of the case and make a determination.

E. Members who remain in LEADSDENY status can no longer perform the functions of a police officer within the Cleveland Division of Police; LEADSDENY status is a Group IV violation pursuant to General Police Order 1.07.06 Disciplinary Guidance and creates the presumption of termination.

V. Physical Protection of CJI

A. CJI shall by protected by the following physical means:

1. Security perimeter.

a. The perimeter of a physically secure location within a Division facility shall be prominently posted and separated from non-secure locations by physical controls.

b. Security perimeters shall be defined, controlled and secured in a manner acceptable to LEADS.

2. Physical access authorizations; except for those areas within the facility officially designated as publicly accessible, the Division shall develop and keep a current

list of personnel with authorized access to the physically secure location or shall issue credentials to authorized personnel.

3. Physical access controls; except for those areas within the facility officially designated as publicly accessible, the Division shall control all physical access points and shall verify individual access authorizations before granting access.

4. Access control for transmission medium; except for those areas within the facility officially designated as publicly accessible, the Division shall verify individual access authorizations before granting access.

5. Access control for display medium; the Division shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

6. Monitoring physical access; the Division and Public Safety IT shall monitor physical access to the information system to detect and respond to physical security incidents.

7. Visitor control.

   a. Except for those areas within the facility officially designated as publicly accessible, the Division shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location.

   b. The Division shall escort visitors at all times and monitor visitor activity.

8. Delivery and removal; the Division and Public Safety IT shall authorize and control information system related items entering and exiting the physically secure location.

B. If the Division cannot meet all the controls required for establishing a physically secure location (e.g., City Hall, Mounted Unit, Cleveland Hopkins International Airport, etc.) but has an operational need to access or store CJI, the Division shall designate an area, a room, or a storage container, as a controlled area for the purpose of day to day CJI access or storage, and at a minimum shall:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.

2. Lock the area, room, or storage container when unattended.

3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.

4. Follow the encryption requirements found in Section 5.10.1.2 of the LEADS Security Policy for electronic storage of CJI (i.e., data “at rest”).

VI. Physical and Digital Media Security, Protection, Storage and Transportation

A. The responsibility for the security and protection of information obtained from the LEADS/NCIC/LERMS/FBR computer systems rests with all authorized users that obtain and use the information, as well as the agency receiving such information.

1. Authorized Division members shall protect and control electronic and physical LEADS/NCIC information while at rest and in transit.

2. The Division shall take appropriate safeguards for protecting LEADS/NCIC information to limit potential mishandling or loss while being stored, accessed, or transported.

B. To protect LEADS/NCIC/LERMS/FBR CJI information, Division members, City employees, and vendors working inside a physically secure location within a Cleveland Division of Police facility or on an information system/network shall:

1. Securely store electronic and physical media within a physically secure or controlled location (e.g., a locked drawer, locked cabinet, locked room, etc.).

2. Restrict access to electronic and physical media to authorized individuals only.

3. Ensure that only authorized users remove printed forms or digital media from LEADS/NCIC/LERMS/FBR.

4. Physically protect LEADS/NCIC/LERMS/FBR information until the information is destroyed or sanitized using approved equipment and techniques

5. LEADS/NCIC printouts cannot be left unsupervised while physical controls are not in place; precautions shall be taken to obscure LEADS/NCIC information from public view.

6. Not use personally owned information systems to access, process, store, or transmit CJI.

7. Not utilize publicly accessible computers (e.g., hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.) to access, process, store, or transmit CJI.

8. Store all hard copy CJI printouts maintained by Division in a secure area accessible to only those members whose job function requires them to handle such documents.

C. When not in a secure area, take appropriate action when in possession of CJI.

1. CJI must not leave the member's immediate control, and CJI printouts cannot be left unsupervised while physical controls are not in place.

2. When CCH record information is provided to any *third party* criminal justice agency or person within the criminal justice system, the authorized operator shall enter the name of the requester in the computer check logbook and sign the dissemination log; when exchanging LEADS/LERMS/FBR information between members of the Division, no log is required.

3. The Division shall retain computer check logbooks for the remainder of the year plus an additional six years; logbooks shall be made available upon request to the Bureau of Compliance, BCI, Ohio State Highway Patrol (OSHP), LEADS, LEADS TAC, and the FBI.

4. Precautions shall be taken to obscure CJI from public view (i.e., an opaque file folder or envelope for hard copy printouts, session locks and/or privacy screens for computers or other electronic devices, etc.) and shall not be left in plain public view.

    a. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

    b. When CJI is at rest (stored electronically) outside the boundary of the physically secure location, the data shall be protected; storage devices include external hard drives from computers, printers and copiers used with CJI and include thumb drives, flash drives, back-up tapes, mobile devices, and laptops.

5. Members shall lock or log off computers when not in the immediate vicinity of a work area to protect CJI; all personnel do not have the same CJI access permissions, and CJI shall be protected on a need-to-know basis.

D. Members, City employees, and vendors shall control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Securing hand carried confidential electronic and paper documents.

    a. CJI shall be stored in a locked briefcase, lockbox, or other secure container.

    b. Electronic or printed CJI shall only be viewed or accessed in a physically secure location by authorized personnel.

2. Hard copy printouts or CJI documents shall be packaged in such a way as to not have any CJI information viewable; printout reports, or any other physical media shall be carried in an envelope or folder.

VI. Media Destruction and Sanitation

A. Hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store and/or transmit LEADS/NCIC/LERMS/FBR CJI and classified and sensitive data shall be properly disposed of when no longer needed.

B. Physical media, including printouts and other physical media, shall be disposed of by one of the following methods:

1. Shredding using Division or City issued shredders; if using a City waste management site, a Division member must witness the entire shredding process.

2. Placed in locked shredding bins for approved Division private contractor to come on site and shred, witnessed by a Division member throughout the entire shredding process.
3. Incineration witnessed by a Division member on site at Division or at a contractor incineration site, if conducted by non-authorized personnel.

C. Electronic media (i.e., hard drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the following methods:

1. Overwriting to clear magnetic media by using a program to write 1s, 0s, or a combination of both onto the location of the media where the file to be sanitized is located; overwriting shall be completed at least three times.

2. Degaussing to magnetically erase data from magnetic media.

a. The two types of degaussing are strong magnets and electric degausses.

b. Common magnets (e.g., magnets used to hang a picture) are fairly weak and cannot effectively degauss magnetic media

3. Destruction to physically dismantle magnetic media by methods of crushing, disassembling, incineration, or other means to ensure the platters have been physically destroyed so that no data can be obtained.

D. 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 Division or Public Safety IT Department control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

THIS ORDER SUPERSEDES ANY PREVIOUSLY ISSUED DIRECTIVE OR POLICY FOR THIS SUBJECT AND WILL REMAIN EFFECTIVE UNTIL RESCINDED OR SUPERSEDED.

DAD/rs/lms
LEADS Unit
Revised 8/5/22; replaces 3/1/02