N-DEx: Quick Study Guide for Certification

N-DEx – Purpose

- The purpose of N-DEx is to share complete, accurate, timely and useful enforcement/criminal justice information across jurisdictional boundaries and to provide new investigative tools that enhance the nation's ability to fight crime and terrorism.
- The N-DEx Policy and Operating Manual is the minimum N-DEx policy standard. A participating agency may incorporate agency specific policies and procedures; however, no agency policy shall detract from that contained in the manual.
- The N-DEx Policy and Operating Manual applies to all entities with access to, or operating in support of, N-DEx services and information.

N-DEx – Operational Framework

- Participating agencies and users must adhere to the CJIS Policy located in Law Enforcement On-Line (LEO), www.leo.gov.
- N-DEx data is restricted to documented criminal justice information, obtained by criminal justice agencies in connection with their official duties administering criminal justice.
- N-DEx will not contain criminal intelligence data as defined by *Title 28, Code of Federal Regulations (C.F.R.), Part 23*.
- The N-DEx system access is restricted to "criminal justice agencies" and agencies performing the "administration of criminal justice", in accordance with the CJIS Security Policy and consistent with *Title 28, C.F.R, Part 20, Subpart A*.
- Participating agencies contribute information to N-DEx with an express promise of confidentiality.
- By contributing information and allowing access to that information via N-DEx, participating agencies agree to permit the access, dissemination and/or use of such information by other parties according to provisions set forth in the N-Dex Policy and Operating Manual. Each record-owning agency has the sole responsibility and accountability for ensuring that it is not constrained from permitting such access by any laws, regulations, polices or procedures.

N-DEx – Data Use

N-DEx access is based on the CJIS assigned agency Originating Identifier (ORI). Specifically, the following agency types may be granted N-DEx system access:

Law Enforcement Agencies

- Law enforcement agencies possessing 9th character ORIs of 0-9 (numeric value).

Criminal Justice Agencies

- Prosecuting Attorney's Offices – ORIs end in an "A".
- Pretrial service agencies and pretrial release agencies – ORIs end in a "B".
- Correctional institutions – ORIs end in a "C".
- Nongovernmental railroad or campus police departments qualifying for access to III – ORIs end in an "E".
- Probation and Parole Offices – ORIs end in a "J".
- Custodial facilities in medical or psychiatric institutions and some medical examiners' offices which are criminal justice in function – ORIs end in an "M".
- Regional dispatch centers that are criminal justice agencies or noncriminal justice governmental agencies performing criminal justice dispatching functions for criminal justice agencies – ORIs end on an "N".
- Local, county, state of federal agencies that are classified as criminal justice agencies by statute but do not fall into one of the aforementioned categories – ORIs end in a "Y".

Full N-DEx system participants are local, state, tribal and federal criminal justice agencies throughout the United States, District of Columbia and United States territories.

Limited system participants are foreign criminal justice agencies, including INTERPOL.

Federal government unclassified N-DEx information can be shared with limited system participants at the discretion of the federal agency.

Local, state and tribal criminal justice agency data will not be shared with limited participants.

Personnel engaged in the following investigative activities may be granted access by the CJIS Systems Agency (CSA) consistent with state laws:

Law enforcement investigations, i.e., to further investigations of criminal behavior based on prior identification of specific criminal activity by an agency with a statutory ability to perform arrest functions.

Pretrial release investigation, i.e., to obtain information about recently arrested defendant's for use in deciding whether conditions are to be set for defendant's release prior to trial, monitor a defendant's compliance with his/her conditions of release during pretrial period , and identify offenses pending adjudication.

Intake investigation, i.e., to conduct prisoner classification and offender risk assessments to safely manage the correction population.

Correctional institution investigation, i.e., to identify and suppress criminal suspects and criminal enterprise organizations operating within correctional systems, prepare for the prosecution of crimes committed within a correctional institution, conduct criminal apprehension efforts of prison escapees, ensure inmates cannot continue their criminal activities through the misuse of visitation or communication privileges, monitor out source supervision and treatment progress, conduct offender travel permit investigations, prepare for prisoner transfer, and conduct pre-release investigation to determine reentry requirements and facilitate release notification.

Pre-sentence investigation, i.e., to identify the risk of re-offense, flight, community, officer and victim safety, identify law enforcement contact not resulting in arrest, identify offenses pending adjudication, and ensue illicit income is not used for bail, bond or criminal defense.

Supervision investigation, i.e., to identify incident information (e.g., personal conduct, contact with LEAs, offenses, gang affiliations, know associates, employment, etc.) constituting a violation of release or supervision conditions, prepare and investigate interstate transfer of adult offenders, facilitate concurrent supervision, conduct risk and needs assessments, facilitate apprehension of absconders, and identify offenses pending adjudication.

Data administration/management, i.e., to perform administrative role responsibilities and conduct searches of record owner contributed data as a part of internal review by a record owner. Responses for this purpose may not be disseminated for any other reason and are limited to that agency's portion of N-DEx contributed records.

Training, i.e., to educate users on the policies, services and capabilities of the N-DEx system utilizing authentic criminal justice information submitted to N-DEx by criminal justice agencies.

- Searches performed via the N-Dex User Interface identity the N-DEx user, requesting agency, and, when provided by the user, the person the search was made "on behalf of".
- N-DEx information may be viewed, output or discussed without advanced authorization of the record-owning agency when viewed, output or discussed within the record-requesting agency and/or within another agency, if the other agency is also authorized for N-DEx access AND is being serviced (pursuant to an Information Exchange Agreement) by the record-requesting agency.
- Advanced Permission from the record-owning agency is required prior to
    - Action upon N-DEx information
    - Reliance upon N-DEx information
    - Secondary dissemination of N-DEx information
    - Publication or preparation of charts based upon N-DEx information
    - Presentations containing N-DEx information
    - Inclusion of N-DEx information into official files
    - Inclusion of N-Dex information in analytical products or other documentation
    - Inclusion of N-DEx information in the judicial, legal, administrative or other criminal justice process
- The advanced permission must describe how N-DEx information may be used.
- Advanced Permission requires that the N-DEx information must be used within the limitations specified by the record-owning agency.
- Advanced Permission requires that reliance or action upon, or secondary dissemination of N-DEx information beyond the original terms requires further permission from the record-owning agency.

Verification Requirement: N-DEx information must be verified with the record-owning agency for timeliness, accuracy and completeness prior to reliance upon, action or secondary dissemination.

- **Timeliness**: Each record-owning agency shall submit data, including any updates or changes to the original submission as often as feasible. Updates or changes shall be executed at least monthly.

- **Accuracy**: Each record-owning agency shall ensure data contributed to N-DEx is synchronized with its own source system records as they are updated/changed.
- **Completeness**: Each record-owning agency should submit as many N-DEx data elements as they have available or are permitted to by law.

Information returned specifically from N-DEx leveraged CJIS System of Service systems (E.g., NCIC and III) may only be used in accordance with the policies governing those specific systems.

- Immediate use of N_DEx information can be made without advanced permission if there is an <u>exigent circumstance:</u>
    - An emergency situation requiring swift action to prevent imminent danger to life or serious damage to property
    - To forestall the imminent escape of a suspect
    - Destruction of evidence
- A record-owning agency shall be immediately notified of any dissemination made as a result of exigent circumstances

N-DEx – Responsibility for Records

- Each record-owning agency controls how and with whom their data is shared, thus retaining responsibility, control and ownership.
- Record-owning agencies shall ensure data contributed to and/or exchanged by N-DEx is unclassified and free of classified national security information.
- Criminal justice agencies that have users connecting to N-Dex through methods that do not permit the capture of N-DEx user information have the ability to generate reports upon request of the state CJIS Systems Agency and/or N-DEx Program Office
- N-DEx is designed to allow record-owning agencies to protect their data in accordance with the laws and policies that govern dissemination and privacy for their jurisdictions
- All data is presumed sharable unless the record-owning agency restricts data access in accordance with their sharing policy
- Record-owning agencies may utilize N-DEx's Agency-Configurable Data Sharing Controls to appropriately protect their data and define how they expose their records to the criminal justice community

N-DEx enables data sharing with the following data item dissemination criteria values:

- GREEN: Green data is fully shareable and viewable
- Yellow: Yellow data is controlled as "pointer-based" data. Pointer-based data consists of only record-owning agency Point of Contact (POC) information.
- RED: Red data is not viewable to any N-DEx user unless he or she is a member of an exception group.

N-DEx – System Description

- Data contributed and/or exchanges via N-DEx is criminal justice information, which contains personally identifiable information (e.g., names, social security numbers), as well as non-identifying descriptive information (e.g., offense location, weapon involved), and may contain criminal history record information as defined *in Title 28, C.F.R, Part 20*. The collection, storage and dissemination of information shall comply with all applicable laws and regulations
- In accordance with the CJIS Security Policy, an information agreement must be signed between the CSA and participating agencies within the CSA's state before exchanging criminal justice information

N-DEx – Policy Management

The CJIS Systems Officer (CSO) or designee shall ensure an N-DEx Agency Coordinator (NAC) is designated within each agency which accesses N-DEx. The NAC serves as the Point-of-Contact for the CSO at the local agency for matters relating to N-DEx. The NAC administers N-DEx within the local agency and oversees the agency's compliance with N-DEx system policies. The NAC may also be the agency's Terminal Agency Coordinator.

- There are several agency roles that are responsible for the management, auditing and training functions of N-DEx for an agency.
    - User administrator
    - Source Data Administrator
    - Audit/Security Administrator
    - Automated Processing Administrator
    - Training Administrator

N-DEx – System Security

- The data stored in the N-DEx system is documented criminal justice information and must be protected to ensure authorized, legal, and efficient dissemination and use.
- It is incumbent upon each N-DEx participating agency to implement procedures to make the N-DEx system secure from any unauthorized use.

N-DEx – Quality Control

- Users, participating agencies and CJIS Systems Agencies share a responsibility to
- Ensure appropriate use, enforce system discipline and security integrity
- Ensure compliance with the CJIS Security Policy and N-DEx Policy and Operating Manual
- Ensure completion of basic security awareness training within six months of initial assignment and biennially thereafter for all personnel who have access to criminal justice information
- Ensure users are trained on N-DEx policy matters, emphasizing data use rules prior to accessing N-DEx and every two years thereafter.