U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Law Enforcement National Data Exchange (N-DEx)

Integration Plan

Law Enforcement Information Exchange National Capital Region (LInX NCR) / Maryland, Virginia, and District of Columbia

Version 1.0

Federal Bureau of Investigation
Criminal Justice Information Services Division

December 23, 2014

Table of Contents

1 Document Overview

The purpose of this document is to provide an overall plan for integrating the Naval Criminal Investigative Service (NCIS) Law Enforcement Information Exchange (LInX) Regional System with the Law Enforcement National Data Exchange (N-DEx) System.

LInX is a regional automated law enforcement sharing system developed by the NCIS. It has been fully operational in some regions since 2003. By design, all of the LInX sites operate to assist law enforcement agencies in solving crime and fighting terrorism. There are currently 10 LInX sites in the United States. They are strategically located to protect Naval assets.

The FBI's Criminal Justice Information Services (CJIS) Division N-DEx is the national law enforcement and criminal justice information sharing system designed to assist criminal justice agencies in solving crime and fighting terrorism by enabling sharing of incident and case reports, incarceration and booking, and probation and parole data.

1.1 CJIS Division Background

The CJIS Division provides state-of-the-art identification and information services to the state, local, tribal, federal, and international criminal justice communities. These services are administered and maintained by the CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) along with its administrator for CJIS information, the CJIS Systems Officer (CSO).

The CJIS Systems include, but are not limited to: Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR); Integrated Automated Fingerprint Identification System (IAFIS); Law Enforcement Online (LEO); National Instant Criminal Background Check System (NICS); and N-DEx.

The purpose of a CSO is to unify responsibility for systems user discipline and to ensure adherence to established national procedures and policies within each signatory state/territory/tribal agency and by each federal user. Pursuant to The Bylaws for the CJIS Advisory Policy Board (APB), the role of the CSO shall not be outsourced. However, the CSO may entrust, or delegate, certain responsibilities.

1.2 Advisory Process

N-DEx Policies are recommended by the FBI CJIS APB and approved by the Director of the FBI. N-DEx is managed by the FBI under a long-standing "shared management" concept, in which state, local, tribal, and federal criminal justice entities participate in formulating operating policies and procedures.

Using this shared management concept, the state governments, through the CSOs, are responsible for implementing, managing, and auditing the N-DEx policy requirements within their states. It is the CSOs who work directly with agencies to coordinate both the submission of data and access to N-DEx. They are ultimately responsible for the administration of CJIS Systems used within their respective states.

2 Policy Review

To integrate LInX with N-DEx, it is important to be sure that both systems have complimentary policies for protection of and access to data. Personnel from the N-DEx Program Office (PO), CJIS Audit Unit (CAU), and CJIS Information Security Office (ISO), have reviewed several of the LInX policy documents and compared them to N-DEx and CJIS Division policy documents. (See Appendix A, at the end of this document)

Based upon these reviews, it appears the main areas (but not limited to) that should be addressed to achieve integration are outlined below.

2.1 CJIS Division Security Policy

The CJIS Division Security Policy defines how CJIS System data must be encrypted/protected when returned to an agency and ultimately made available to an individual user.

The N-DEx PO, CAU, and ISO personnel have reviewed the LInX Regional System polices and operations, the *N-DEx Policy and Operations Manual,* and the *CJIS Division Security Policy Version 5.0 (CSP)*, and have determined that the existing LInX Regional System policies and operations are acceptable to fulfill policy and operational requirements of N-DEx for data submission and access.

FBI CJIS ISO personnel performed a review of the *LInX Information Security Policy (ISSP)*. As a result, the ISO identified some apparent discrepancies between the ISSP and the CSP. These issues are being addressed through a coordinated effort between the CJIS ISO and the LInX Information Assurance (IA) Office, with representation from both the N-DEx and LInX PMO's. The CJIS ISO and LInX IA conducted a comparison of the CSP to the LInX ISSP, which resulted in the following:

- Agreement to include references to the CSP in the ISSP, specifically "shall" statements.
- The short term resolution is for LInX to institute a risk-based (i.e. similar to LEO) authentication.
    - Anticipate risk-based solution to be implemented within six months.
    - Identified need to review if ORIs are tracked. The LInX IA Office has implemented this change and it is currently in operation.
- NCIS Program Management is committed to identifying the security requirements for all LInX regions, and will take responsibility for the resource requirements.

The FBI CJIS ISO office fully concurs with the N-DEx PO's plan to ingest LInX Regional System data into N-DEx and to allow N-DEx data to be viewed by LInX Regional System users immediately.

The FBI CJIS ISO continues to coordinate with the LInX IA office to identify specific areas in the LInX ISSP that may require clarification or modification with regard to the CSP. The CJIS ISO's goal is to work with the LInX IA office to ensure the ISSP and CSP are appropriately synchronized as expeditiously as possible.

2.2 LInX Security Policy

The LInX Regional system has a Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Authority to Operate (ATO).

The DIACAP requirements are more specific than Federal Information Security Management Act (FISMA) requirements.

The CSP 5.0 contains 12 policy areas, and these 12 areas are covered in a DIACAP certification and accreditation assessment.

Initial review indicates that, according to LInX documents, LInX security must be maintained consistent with federal standards so as not to preclude the full participation of DoD, Department of Justice, or Department of Homeland Security agencies. The system must be accredited under the DIACAP standard for sensitive but unclassified law enforcement data.

Access to N-DEx data through a LInX Regional System will be a work in progress as the integration evolves.

2.3 N-DEx Audit Policy

N-DEx use will be audited by the CAU. Specifically, the CJIS auditors will review what queries have been conducted by taking a random sampling of users in each state. As such, based on the current CJIS model, CJIS auditors will work through each state's CSA to audit users.

Currently, LInX users are audited by LInX; however, this action does not fall under the purview of the CSA. Therefore, the CSA must be able to account for not only what a user queries by direct access to the N-DEx System, but also queries through the LInX Regional System whenever N-DEx search results are provided.

A review of LInX audit policies by CAU staff indicates no major concerns with audit procedures. LInX Regional Systems keep an audit log for five years, that capture login and query information. N-DEx captures the user profile information of anyone who queries the N-DEx System, whether it be directly through the N-DEx Portal or through a query from another participating system. This information is provided to the CSA.

LInX Regional Systems shall provide audit logs to N-DEx and the CSA as part of an agreement to move forward.

2.4 Training Policy

LInX users are required to complete training as part of their agency agreement to participate with LInX. Prior to accessing N-DEx, CSA's shall ensure, directly or through local delegation, that users are trained on N-DEx policy matters, emphasizing data use rules. Basic security awareness training shall be required within six months of initial assignment and biennially thereafter for all personnel who have access to N-DEx. The CSA in each respective state may choose to enforce additional training requirements upon users who desire access to N-DEx. The APB is also moving toward a requirement for all N-DEx users to complete training, however, this has not been approved yet. N-DEx computer-based training modules are available on the LEO site, and may also be provided to any agency upon request.

LInX Regional Systems shall modify training requirements to include N-DEx policies.

3 Definition of Integration

Prior to a discussion on how to integrate LInX Regional Systems with N-DEx, it is necessary to define integration. As understood through discussions with N-DEx stakeholders, the LInX stakeholders, and state and local agencies who have a vested interest due to the presence of a LInX Regional system in their state, integration can be summarized as:

- **Data Submission:** To resolve and correlate information from the LInX Regional system with information from the rest of the nation, data must be submitted from the LInX Regional system to the N-DEx system.
- **Data Access:** To create value, Law Enforcement personnel who utilize LInX (those who query and those who contribute their data to share) must be able to interact with and receive data from N-DEx. There are several options for access and several requirements that must be considered to successfully integrate the two systems. (See section 3.3 Access Solution)

3.1 Solution Overview

To accept the definition of integration defined in this document, it is necessary to develop a solution that addresses two major issues along with numerous requirements that must be met to satisfy each. An N-DEx/LInx/CSA Integration Working Group (IWG) will identify the issues that exist for this integration project and will ensure the solution addresses these issues.

3.1.1 Data Submission Overview

This section addresses the first bullet used in defining an integration effort by identifying the major components associated with a large data sharing effort and developing an accepted solution that addresses any concerns.

Why Data Submission

One of the most powerful services that N-DEx provides to the nation is the ability to review information from hundreds of millions of documents, and develop both entity resolutions (N-DEx thinks these four people are really the same person) and entity correlations (N-DEx thinks these two people know each other). Currently, N-DEx is performing this service on approximately 85 million documents consisting of about 500 million entities (people, places, and things).

N-DEx provides a large assortment of resources that are dedicated to the aforementioned analysis 24 hours a day, seven days a week. N-DEx does have the ability to query other operational systems via a Web service; however, due to the vast user base that N-DEx services, this is only practical for systems with the scalability to provide access to hundreds of thousands of users simultaneously. N-DEx currently operates in this manner with NCIC and OneDOJ, and will be adding access to the Department of Homeland Security Law Enforcement Information Sharing Service System very soon. However, N-DEx cannot perform the entity resolution and entity correlation services on data unless that data has been submitted for processing. Furthermore, responses from Web service queries are not saved where they can be further analyzed. They are simply displayed to the N-DEx user at the time of the query.

In short, data is submitted to N-DEx from law enforcement agency systems so that it can be correlated and resolved with data from other agencies, making N-DEx a CJIS System with a high degree of functionality on a 24/7 schedule.

3.1.2 Data Submission Solution

When submitting data to N-DEx, an agency is a data submitter, a data owner, or both. A data submitter is an agency that receives data from all of the data owners and delivers that data to N-DEx, e.g., state agency, regional system. A data owner is an agency that has criminal justice information they want to correlate and resolve against data from other agencies across the country. The data owner sends the data to their data submitting agency for submission to N-DEx. The diagram below illustrates this model as typically seen utilized as part of a state network, i.e., NCIC.

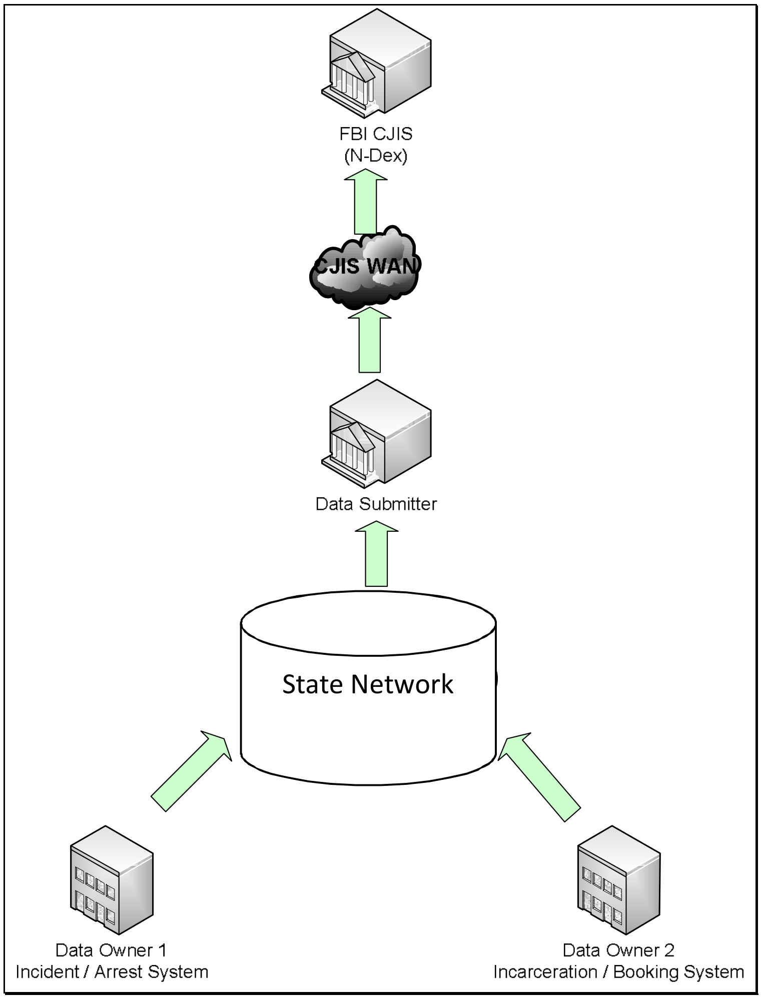


Figure 1: N-DEx Data Submission Model

The LInX Regional System is what is commonly referred to as an aggregator. The data that is already "aggregated" in the LInX Regional System exists in a Law Enforcement Exchange Specification (LEXS) format, in Extensible Markup Language (XML) that is acceptable in its current state for inclusion in the N-DEx System. This model provides a secure, single point of connection to transmit records from the LInX member agencies directly to N-DEx, with little impact on the CSA's resources. The diagram below illustrates a model for a LInX Regional System as a data submitter.

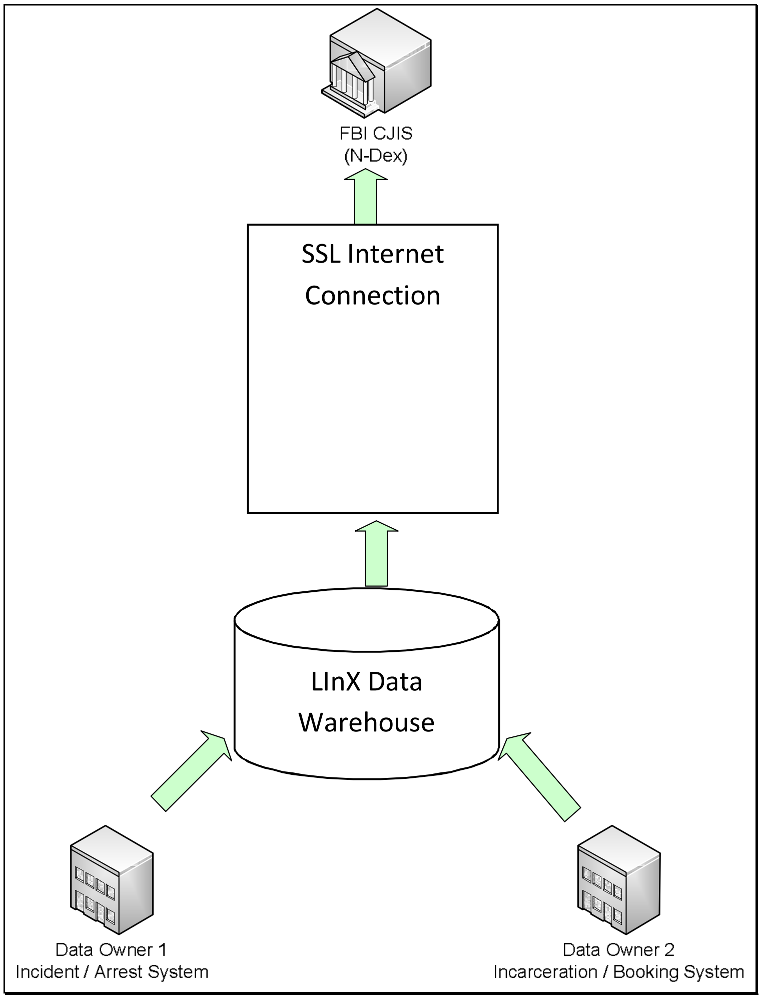


Figure 2: LInX Data Submission Model

Note: A Secure Socket Layer (SSL) connection uses cryptographic protocols that provide communications security over the Internet.

N-DEx is incorporating the above model for data submission in many criminal justice agencies across the country, where aggregation points exist separately from the state network. There are several reasons to consider this option:

- The state agency has no centralized warehouse or state system.
- The state does not desire to collect the information being aggregated locally/regionally.

- The state already has access to the local data and has no issue with how the data is submitted.
- It makes operational sense to obtain the data from a regional system.

3.2 N-DEx Access Overview

Historically, access to CJIS Systems has been handled through a state message switch at each CSA. Each state agrees to be responsible for the security of and access to CJIS data by signing a User Agreement with the CJIS Division. In turn, the state has agreements with the local agencies requiring them to adhere to all CJIS Division and State polices.

As technology bounds forward, new ways of accessing CJIS data have come to fruition. With the delivery of N-DEx, as well as new and improved methods for sharing information, there are multiple ways of accessing data. As such, requirements for protecting that data must be met.

3.3 Access Solution

In today's environment, users obtain information from a variety of interfaces and mechanisms. In almost every work environment, users are accustomed to a certain set of tools and information delivery mechanisms. For this reason, N-DEx must be able to deliver information in a variety of ways. This section describes a subset of those mechanisms that are proposed to be used by LInX sites.

3.3.1 Direct Access to N-DEx Portal via hyperlink on LInX portal

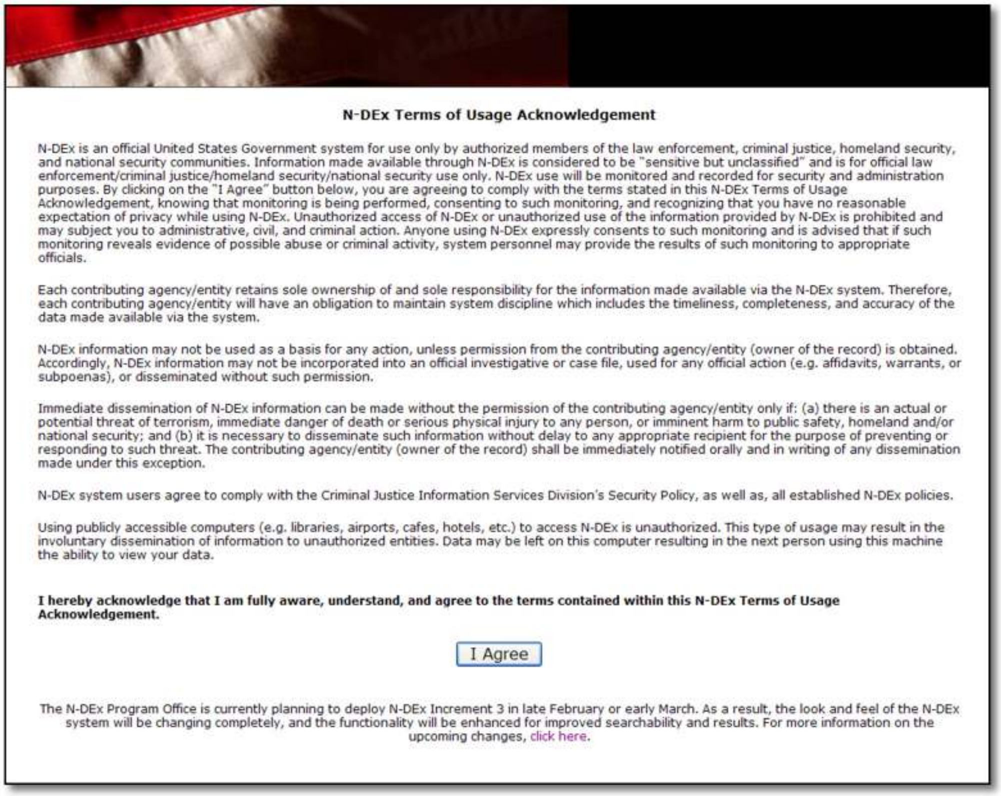
Many N-DEx users want to log directly into the N-DEx portal, but do not want to get a LEO account. Instead, they want to use one of their existing accounts to log directly into the N-DEx portal. N-DEx has the ability to trust an agency's existing identity management solution.

Example – LinX user accessing N-DEx Portal

Step 1: User logs into LInX

Step 2: User clicks the "N-DEx" link on the LInX portal.

Step 3: User sees the N-DEx Portal (below)



N-DEx Terms of Usage Acknowledgement

N-DEx is an official United States Government system for use only by authorized members of the law enforcement, criminal justice, homeland security, and national security communities. Information made available through N-DEx is considered to be "sensitive but unclassified" and is for official law enforcement/criminal justice/homeland security/national security use only. N-DEx use will be monitored and recorded for security and administration purposes. By clicking on the "I Agree" button below, you are agreeing to comply with the terms stated in this N-DEx Terms of Usage Acknowledgement, knowing that monitoring is being performed, consenting to such monitoring, and recognizing that you have no reasonable expectation of privacy while using N-DEx. Unauthorized access of N-DEx or unauthorized use of the information provided by N-DEx is prohibited and may subject you to administrative, civil, and criminal action. Anyone using N-DEx expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

Each contributing agency/entity retains sole ownership of and sole responsibility for the information made available via the N-DEx system. Therefore, each contributing agency/entity will have an obligation to maintain system discipline which includes the timeliness, completeness, and accuracy of the data made available via the system.

N-DEx information may not be used as a basis for any action, unless permission from the contributing agency/entity (owner of the record) is obtained. Accordingly, N-DEx information may not be incorporated into an official investigative or case file, used for any official action (e.g. affidavits, warrants, or subpoenas), or disseminated without such permission.

Immediate dissemination of N-DEx information can be made without the permission of the contributing agency/entity only if: (a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to public safety, homeland and/or national security; and (b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such threat. The contributing agency/entity (owner of the record) shall be immediately notified orally and in writing of any dissemination made under this exception.

N-DEx system users agree to comply with the Criminal Justice Information Services Division's Security Policy, as well as, all established N-DEx policies.

Using publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access N-DEx is unauthorized. This type of usage may result in the involuntary dissemination of information to unauthorized entities. Data may be left on this computer resulting in the next person using this machine the ability to view your data.

I hereby acknowledge that I am fully aware, understand, and agree to the terms contained within this N-DEx Terms of Usage Acknowledgement.

The N-DEx Program Office is currently planning to deploy N-DEx Increment 3 in late February or early March. As a result, the look and feel of the N-DEx system will be changing completely, and the functionality will be enhanced for improved searchability and results. For more information on the upcoming changes, click here.

Figure 3: N-DEx Warning Banner

Advantages

- Users can view N-DEx data directly from the N-DEx portal with their existing LInX account.
- Users will be able to access all of the N-DEx tools, i.e. visualization, subscription, collaboration, etc. that are available within the system.
- Access can be managed and easily granted based on best practices.

Disadvantages

- If used without the LEXS-SR interface, users will have to perform separate queries of LInX and N-DEx because each system will provide standalone results.

3.3.2 Query N-DEx from LInX Portal (LEXS SR)

In addition to the portal access, LInX users need the ability to have the LInX system query N-DEx and return the search results into their LInX application. This functionality is provided via the N-DEx LEXS-SR interface.

Advantages

- Many users are comfortable with their existing interface for investigative analysis work.
- Agencies can set up their IT systems to query N-DEx via Web services, and incorporate the search results into their home portal.
- Access can be managed and easily granted based on existing best practices.

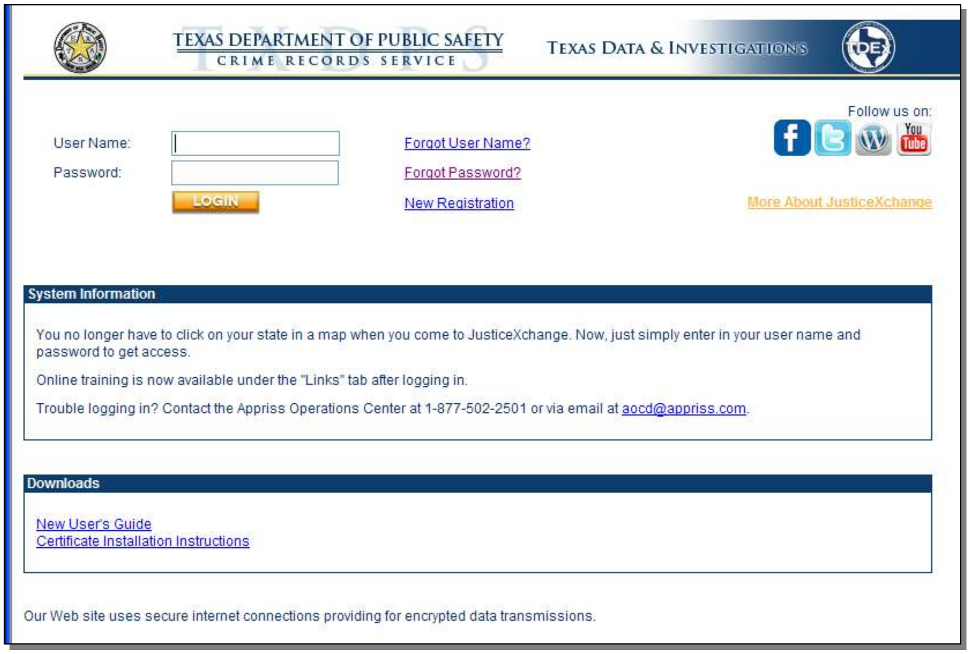
Disadvantages

- There is a limitation of searching N-DEx in this manner; there is no access to the tools within N-DEx, i.e., Subscription, Notification, Collaboration. The data returned is a subset of what is actually in N-DEx, so a user who needs to "drill down" into the data for more in-depth analysis would have to access the N-DEx System via the N-DEx Hyperlink to do so.
- Users must be trained, notified of the Rules of Behavior, security policies, etc. for access to N-DEx data and reminded that they are accessing a CJIS System.
- Tracking of queries must be pulled from both systems' Audit logs.
- Additional work may be required by an agency to display the results within their system's interface.

Note: This method is already being used in Texas with the Texas Data Exchange (T-DEx), San Diego with the Automated Regional Justice Information System (ARJIS), the New Jersey State Police, and at the federal level with OneDOJ.

Following is an example of the LEXS-SR access implemented at T-DEx:

Step 1: User logs into T-DEx (For example)


TEXAS DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS SERVICE
TEXAS DATA & INVESTIGATIONS
TDEx

User Name:

Password:

LOGIN

Forgot User Name?

Forgot Password?

New Registration

Follow us on:

More About JusticeXchange

System Information

You no longer have to click on your state in a map when you come to JusticeXchange. Now, just simply enter in your user name and password to get access.

Online training is now available under the "Links" tab after logging in.

Trouble logging in? Contact the Appriss Operations Center at 1-877-502-2501 or via email at aocd@appriss.com.

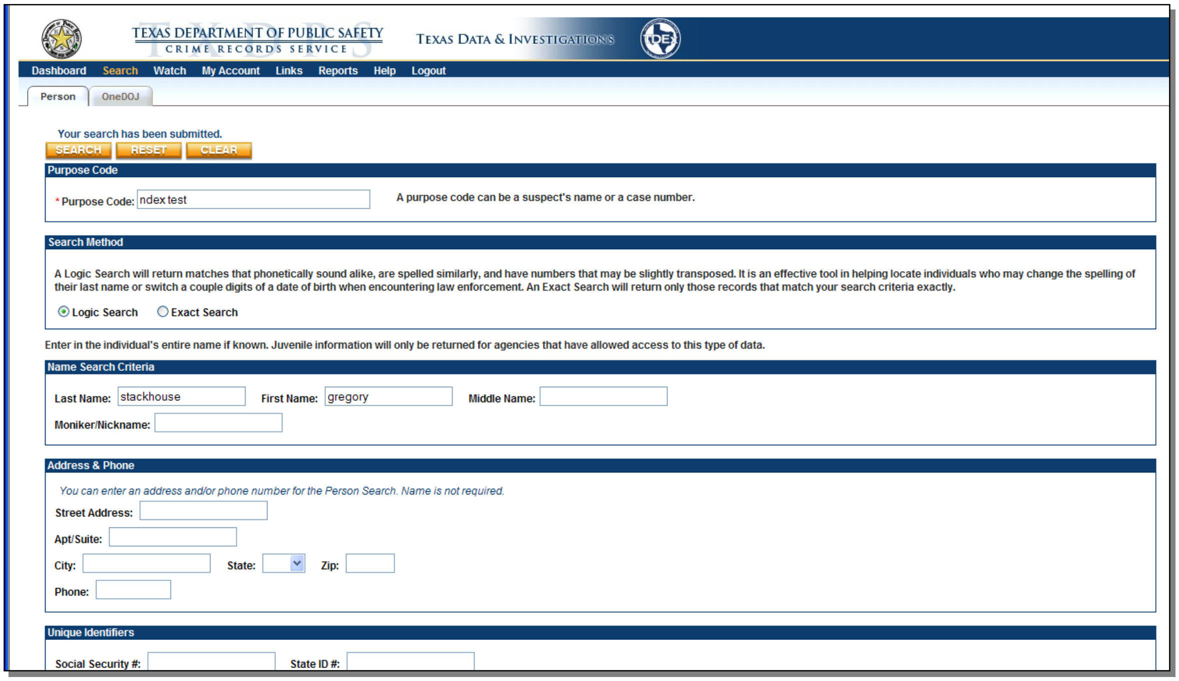
Downloads

New User's Guide
Certificate Installation Instructions

Our Web site uses secure internet connections providing for encrypted data transmissions.

Figure 4: T-DEx Login Screen

Step 2: User performs a T-DEx / N-DEx search



Your search has been submitted.

Purpose Code

* Purpose Code: ndex test

A purpose code can be a suspect's name or a case number.

Search Method

A Logic Search will return matches that phonetically sound alike, are spelled similarly, and have numbers that may be slightly transposed. It is an effective tool in helping locate individuals who may change the spelling of their last name or switch a couple digits of a date of birth when encountering law enforcement. An Exact Search will return only those records that match your search criteria exactly.

● Logic Search ○ Exact Search

Enter in the individual's entire name if known. Juvenile information will only be returned for agencies that have allowed access to this type of data.

Name Search Criteria

Last Name: stackhouse First Name: gregory Middle Name:

Moniker/Nickname:

Address & Phone

You can enter an address and/or phone number for the Person Search. Name is not required.

Street Address:

Apt/Suite:

City: State: Zip:

Phone:

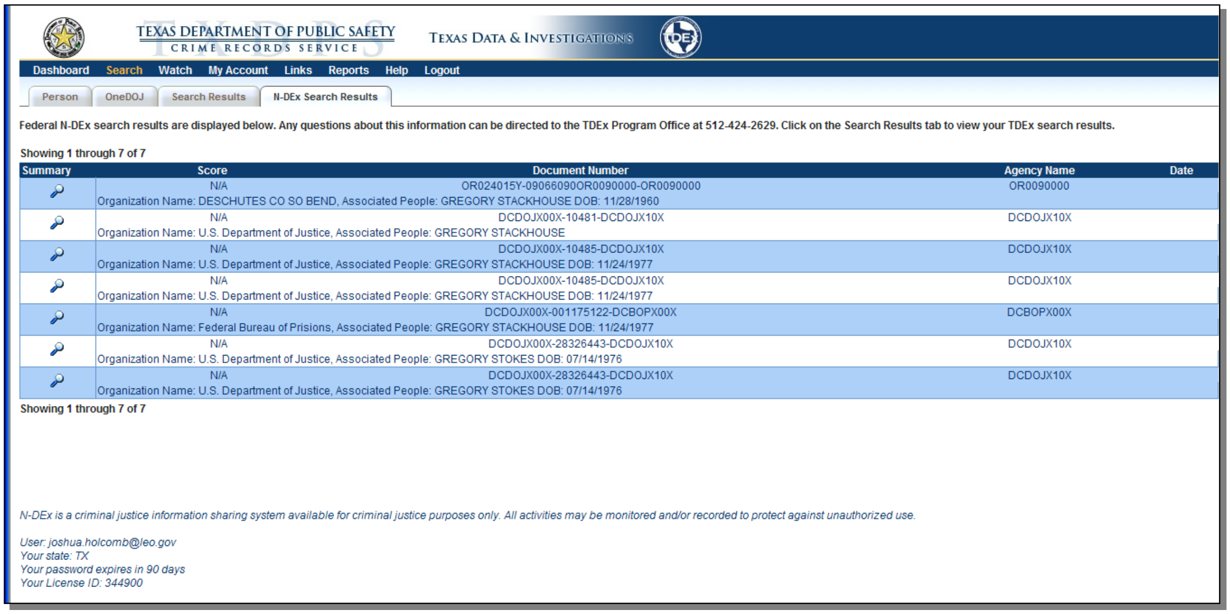
Unique Identifiers

Social Security #: State ID #:

Figure 5: T-DEx Search Screen

Search results for T-DEx are displayed on the search results tab

Search results for N-DEx are displayed on the N-DEx tab. This method results in two different sets of results that the user must review.



Federal N-DEx search results are displayed below. Any questions about this information can be directed to the TDEx Program Office at 512-424-2629. Click on the Search Results tab to view your TDEx search results.

Showing 1 through 7 of 7

Summary	Score	Document Number	Agency Name	Date
🔍	N/A Organization Name: DESCHUTES CO SO BEND, Associated People: GREGORY STACKHOUSE DOB: 11/28/1960	OR024015Y-09066090OR0090000-OR0090000	OR0090000	
🔍	N/A Organization Name: U.S. Department of Justice, Associated People: GREGORY STACKHOUSE	DCDOJX00X-10481-DCDOJX10X	DCDOJX10X	
🔍	N/A Organization Name: U.S. Department of Justice, Associated People: GREGORY STACKHOUSE DOB: 11/24/1977	DCDOJX00X-10485-DCDOJX10X	DCDOJX10X	
🔍	N/A Organization Name: U.S. Department of Justice, Associated People: GREGORY STACKHOUSE DOB: 11/24/1977	DCDOJX00X-10485-DCDOJX10X	DCDOJX10X	
🔍	N/A Organization Name: Federal Bureau of Prisions, Associated People: GREGORY STACKHOUSE DOB: 11/24/1977	DCDOJX00X-001175122-DCBOPX00X	DCBOPX00X	
🔍	N/A Organization Name: U.S. Department of Justice, Associated People: GREGORY STOKES DOB: 07/14/1976	DCDOJX00X-28326443-DCDOJX10X	DCDOJX10X	
🔍	N/A Organization Name: U.S. Department of Justice, Associated People: GREGORY STOKES DOB: 07/14/1976	DCDOJX00X-28326443-DCDOJX10X	DCDOJX10X	

Showing 1 through 7 of 7

N-DEx is a criminal justice information sharing system available for criminal justice purposes only. All activities may be monitored and/or recorded to protect against unauthorized use.

User: joshua.holcomb@leo.gov
Your state: TX
Your password expires in 90 days
Your License ID: 344900

Figure 6: N-DEx Search Results via T-DEx

4 Conclusion

To successfully integrate LInX Regional Systems with N-DEx, many data submission and data access issues must be resolved. Data submission directly from the LInX Regional system to the N-DEx system makes practical and operational sense for the following reasons:

- The data in LInX Regional System is already formatted for direct ingestion into N-DEx
- The LInX Regional System has agreed to make the data available to N-DEx in a timely manner and to follow the N-DEx data submission policy.

User access through an N-DEx hyperlink or a LEXS SR connection, in conjunction with approval of applications through the N-DEx application process using LEO, and eventually EIMS are also viable solutions for the following reasons:

- The LInX Regional System users are already familiar with the LInX interface and will need minimal training to make effective use of the N-DEx data.
- The LInX Regional System executive staff agree to make training, audit, and notification of N-DEx Rules of Behavior and use of N-DEx data a part of their own LInX Regional System requirements.
- The LInX Regional System Law Enforcement partners will immediately reap the benefits of access to 85 million records from state, local, tribal, and federal agencies, to which they do not currently have access.
- Additional access methods are possible at the CSA, regional system, or local agencies upon request and per approval of the CSA.

All parties involved must have the proper tools and resources at their disposal to conduct business in the most effective and efficient manner. The following discussion points are provided as an example for integration consideration.

1. Training: Prior to accessing N-DEx, CSA's shall ensure, directly or through local delegation, that users are trained on N-DEx policy matters, emphasizing data use rules. Basic security awareness training shall be required within six months of initial assignment and biennially thereafter for all personnel who have access to N-DEx. The CSA in each respective state may choose to enforce additional training requirements upon users who desire access to N-DEx. The APB is also moving toward a requirement for all N-DEx users to complete training, however, this has not been approved yet. N-DEx computer-based training modules remain optional, but are highly recommended.

    a. The LInX Regional System member agencies shall ensure that the required training takes place. When additional training requirements are established for N-DEx; the LInX Regional System, its member agencies, CJIS, and the CSAs will work together to address how those requirements are fulfilled.

   b. The LInX Regional System member agencies shall provide a list of persons who have been trained upon request by the CSAs or N-DEx Program Office. These lists will be used for audit purposes.

   c. N-DEx provides to the LInX Regional System all Computer Based Training modules and other training materials developed for CSAs and local agencies. These materials will be made available to the member agencies in the LInX Region.

2. Audit: The present N-DEx auditing requirement stipulates that the FBI will include N-DEx system use audits in their triennial audits of CSAs. In addition, CSAs are required to audit N-DEx participation by user agencies in their state separately from the FBI CAU process.

   a. The LInX Regional System shall include appropriate questions addressing N-DEx use in their audit process.

   b. The LInX Regional System shall advise their member agencies that CJIS and the CSAs may audit their use of N-DEx through The LInX Regional System, and may need access to The LInX Regional System audit reports currently utilized and those implemented in the future.

   c. The LInX Regional System member agencies shall provide CJIS and the CSAs with the LInX Regional System transaction reports necessary for the FBI and the CSAs to perform auditing of N-DEx use through the LInX Regional System.

   d. N-DEx provides appropriate questions to the LInX Regional System for inclusion in the LInX audits.

3. User Management: The present N-DEx User Management requirements include fingerprint background checks, training on system use and dissemination, and limiting access only to authorized individuals.

   a. The LInX Regional System shall notify the CSAs when new agencies begin to participate in N-DEx through the LInX Regional System, both when they begin to submit data to N-DEx through the LInX Regional System and when they are authorized for query access to N-DEx through the LInX Regional System.

   b. The CSA's shall provide and maintain current contact information for the LInX Regional System to utilize for contacting the CSA.

   c. The LInX Regional System annually, or upon request, shall provide the CSAs with user lists of persons in their states accessing N-DEx through the LInX Regional System.

4. Security Violations: N-DEx was developed with privacy and security in mind, and each participating agency must ensure that access to N-DEx information is on a strictly need-to-know basis, and that all information is treated as sensitive. All CJIS systems require that the CSA of the respective state be notified of system violations.

   a. The LInX Regional System shall notify CJIS and the appropriate CSAs of any violations of security, dissemination, incorrect use, or other policy that creates vulnerability or compromises N-DEx or the information derived from N-DEx. The notification includes a description of the incident.

b. The LInX Regional System shall provide, or ensure the local agency provides, the affected CSAs with a written statement of the resolution of the incident.

c. The CSAs will remain in contact with the LInX Regional System and the member agency on the violation and may follow up with the CAU, the LInX Regional System, and the violating agency directly.

Never before has the need to share information, leverage existing resources, and to “know what you don’t know” been as great as it is today. With ever decreasing resources and added responsibilities, criminal justice agencies must work harder than ever to fight crime and terrorism. By combining resources, LInX, CSA’s, and N-DEx can work to accomplish this mission by automating work and providing investigative leads to users in the criminal justice community.

Appendix A

- HR LInX Audit Policy v2.0 Adopted 9/10/2008
- HR LInX Oversight Committee Policy v2.0 Adopted 9/10/2008
- HR LInX Rules of Operation Adopted June 9 2004
- LInX Rules of Operation (Jessup) May 2005
- LInX NW Rules of Operation NOV 2006
- Audit Checklist LInX NW 2010
- LInX User Operations Guide Preview
- LInX Oversight Committee Operational Guidelines
- LInX Disclosure of Information Protocol
- SSAA Appendix H – Security Policy
- SSAA Appendix I – Interconnection Security Agreements
- Revised Access and User Agreement LInX