



Law Enforcement National Data Exchange



Data Submission and Connectivity Guide For Law Enforcement Agencies

N-DEX-DOC - 09102 – 1.0

Document Date: March 10, 2008



Table of Contents

1	Document Purpose	3
2	Data Submission	3
2.1	Prerequisites for Data Submission	3
2.2	Data Formatting	4
3	N-DEx Connectivity Overview	4
3.1	Direct Connection via the CJIS WAN	5
3.2	VPN Connection via the Internet	5
3.3	N-DEx DEBUG Overview	5
3.4	N-DEx DEBUG Connectivity	6
3.5	N-DEx DEBUG Interfaces	6
3.6	Submission Methods	6
3.6.1	Manual Submission	6
3.6.2	Batch Submission Process	7
3.6.3	Web Services Submission Process	8
3.6.4	Incident Submission via N-DEx Portal	9
4	Initial Legacy Data Submission	9

1 Document Purpose

The purpose of this document is to provide Law Enforcement Agencies (LEAs) with an informational overview for connecting to the N-DEx system and submitting data. This document is intended to supplement guidance through your liaison representative, serving as a roadmap for establishing connectivity and contributing data to N-DEx. The intended audience for this document is agency officials and their technical personnel.

2 Data Submission

2.1 Prerequisites for Data Submission

The following prerequisites must be in place in order for N-DEx to accept your data:

1. The Operational Memorandum of Understanding must be signed and returned.
2. During Increment 1 N-DEx focuses on incident information and can currently accept data that is formatted in the N-DEx IEPD.
 - a. The most current data specification can be found through the following link: http://it.ojp.gov/jsr/common/viewDetail.jsp?sub_id=240&terms
3. Data files have passed a structural verification and content review.
 - o The N-DEx Data Standards Team uses the ConTesA conformance tool.
 - o It is highly recommended that the test data first be tested with the N-DEx ConTesA tool.
4. File Names adhere to the following naming convention:
 - a. AAAAAAAAAA_YYYYMMDD_HHMM_NNNN.xml, where AAAAAAAAAA is the Data Submitter Agency ORI, YYYYMMDD is the 4-digit year, 2-digit month, and 2-digit day, HHMM is the 2-digit hour (24 hour clock) and 2-digit minute, and NNNN is a 4-digit sequence number. The date and time in the file name should be the creation date and time of the xml file. The sequence number is used to guarantee unique file names. The LEA System is responsible for making sure the files are named uniquely. A sample filename for second file created by a Data Submitter Agency with ORI 'ORIPD0001' at 1:02 pm on March 9, 2007 is 'ORIPD0001_20070309_1302_0002.xml'.
5. File Size

NOTE: .xml file = Xml Document Instance

XML Document sizing recommendations

- o 2000 package maximum in a single XML Document Instance (for i.e. WVNDX0000_20080130_1201_0001.xml)
- o 70 MB maximum file size for a single XML Document Instance
- o 12 Total attachments inside a single XML Document Instance (for i.e. if I have an .xml file, with 1 or 1000 packages, I can only have a maximum of 12 attachments in the file)

Zip file sizes for batch ingest

- o see prerequisite XML Document Instance constraints above
- o Maximum of 20,000 .xml files in a single .zip file. Each XML Document Instance (file) would only have a single message and package
- o 2 GB maximum file size for a single .zip file

2.2 Data Formatting

In order for the N-DEx to receive a system's information, it must first be formatted according to the N-DEx specification for data submission. Therefore, you will be required to format your system's data according to an approved N-DEx submission specification.

During Increment 1 N-DEx focuses on incident information and can currently accept data that is formatted in the N-DEx IEPD. If the LEA's technical personnel need assistance with data formatting, please contact your liaison specialist. The N-DEx IEPD can be downloaded at http://it.ojp.gov/jsr/common/viewDetail.jsp?sub_id=240&terms.

N-DEx IEPD V1.0.1 – The N-DEx IEPD V1.0.1 was generated by the N-DEx program office and Georgia Tech Research Institute (GTRI), and is based on NIEM 1.0.

3 N-DEx Connectivity Overview

Connectivity to the N-DEx system is achieved using the LEA's existing CJIS WAN connection or via an Internet based virtual private network (VPN) connection to CJIS. In the event that a CJIS WAN circuit is not available, the LEA will have to use a VPN over the Internet to achieve connectivity. Below is a list of what each connection requires:

- CJIS WAN Connection
 - o The LEA must have an existing CJIS WAN connection
 - o It is recommended the LEA's CJIS WAN connection be greater than 56k
- VPN Connection over the Internet
 - o The LEA must have an Internet connection
 - o The LEA must provide a Cisco VPN termination endpoint
 - o The VPN must support 3DES or AES encryption

Initial connectivity for data submission will be to the N-DEx debug area. N-DEx will offer a debug area that will allow partnering systems to test their data formatting and network interfaces before submitting data into the operational environment. After the

LEA has performed data tests for validation; submission to the N-DEx Operational Environment can occur.

Your agency will work with an N-DEx liaison specialist to establish connectivity to the N-DEx system. The first step is to complete a connectivity checklist which will be provided by your liaison specialist. Once the connectivity checklist is returned to the liaison specialist, it must be reviewed by an internal FBI technical review board. The results of this board will be the decision to allow connectivity and the connectivity method used. This process can take up to three weeks. Upon board approval, the liaison specialist will schedule a teleconference involving technical representation from your agency and N-DEx to coordinate the technical details involved in establishing connectivity.

3.1 Direct Connection via the CJIS WAN

The CJIS WAN uses leased lines for point-to-point connection between the FBI CJIS Division and its customers. LEAs that have an established CJIS WAN line may be able to use that line for N-DEx data submissions. CJIS will conduct a technical analysis of the line to determine bandwidth utilization requirements, based on the current line usage.

3.2 VPN Connection via the Internet

Connectivity can be established via a virtual private network (VPN) connection over the Internet. This is the preferred method for LEAs that do not have an existing CJIS WAN connection already in place or are restricted from using their CJIS WAN connection for N-DEx data submission. It is recommended that your Internet connection have a minimum bandwidth of 512 kbps in order to utilize a VPN solution. In addition, network hardware must be a Cisco device that supports VPN termination and 3DES or AES encryption. Technical representatives from N-DEx and your agency will coordinate connectivity, which involves:

- Configuration of peer address at the LEA;
- Exchange of VPN key pairs between the LEA and N-DEx
- Test the LEA VPN endpoint to see if the VPN tunnel will build.

3.3 N-DEx DEBUG Overview

The N-DEx DEBUG environment will be provided to all partnering LEAs when they request access to N-DEx. This “practice” area will provide partners of N-DEx with an environment to test data submissions, validate data formats, and implement security mechanisms before their agency is connected to the operational system. Using this environment, agencies can experiment with N-DEx interfaces without fear of contaminating the operational system with test data.

3.4 N-DEx DEBUG Connectivity

When an agency requests to be connected to N-DEx, FBI CJIS personnel will create work orders to connect the requesting agency to both the N-DEx DEBUG area and the N-DEx operational environment. However, access to the N-DEx operational environment will be restricted until the agency tests data submissions against the N-DEx DEBUG area to validate their data format and verify that their security mechanisms are working correctly.

Once the agency has successfully tested in the DEBUG environment, they can call their liaison to request access to the operational environment. Once access is granted by the N-DEx staff, the agency will need to move their data submission targets to the operational system.

3.5 N-DEx DEBUG Interfaces

The N-DEx DEBUG environment will offer both SFTP and web service interfaces for data submissions. These interfaces will mirror those on the operational system, and will return responses regarding the success or failure of a data submission as the operational system does.

3.6 Submission Methods

N-DEx supports four separate mechanisms for transferring data from its partnering agencies to the N-DEx system. Once an agency's initial dataset has been submitted to N-DEx and processed by the system, data submissions can be transferred to the N-DEx system via Manual Submission, SFTP, Web Services, or via typing the incident report into the N-DEx portal. The following paragraphs will discuss each of these transfer mechanisms in more detail.

3.6.1 Manual Submission

The manual data submission process is used when the LEA does not have a means to electronically submit data to N-DEx. The LEA can send the data on an external media device. All data on the external media device must be encrypted before being sent to CJIS. The method for decryption must be discussed with the CJIS technical staff during the technical teleconference. Manual submission data must be sent using a secure method (i.e. Federal Express). The following steps provide greater detail for manually submitting data.

1. It is assumed the LEA has already mapped their data to the N-DEx Information Exchange Package Documentation (IEPD). It is also assumed the agency has conducted XML structural verification checks as per the National Information Exchange Model (NIEM), the Law Enforcement Information Sharing Program Exchange Specification (LEXS), and the N-DEx IEPD conformance.
 - a. The N-DEx IEPD is located online:
http://it.ojp.gov/jsr/common/viewDetail.jsp?sub_id=240

- b. A conformance tool, Conformance Testing Assistance (ConTesA), is available to implementing agencies for structural review of their submissions. ConTesA is located at: <http://ngqt.swbs.gtri.gatech.edu/N-DEx>. The LEA requests access to ConTesA through their N-DEx Liaison Specialist (LS).
- 2. Compress (zip) the files.
- 3. The LEA copies their arrest/incident files onto external media.
- 4. The LEA encrypts the data on the external media device
- 5. The LEA submits their data to CJIS:
 - a. Electronically by email to the LS assigned to the LEA's territory. Files cannot be larger than 7 megabytes in size when submitting to a LEO email address. If you are submitting your data via LEO, work closely with your Liaison to achieve successful handoff.
 - b. By Fed-Ex to address:
 - FBI CJIS Division
 - Attention: N-DEx Data Submissions
 - Module B-3
 - 1000 Custer Hollow Road
 - Clarksburg, WV 26306
- 6. Once the data is received by the N-DEx Program Office, the data will be ingested into the N-DEx system. After the data has been ingested into N-DEx, an email will be sent back to the LEA stating that the data has been processed.

3.6.2 Batch Submission Process

Batch submission refers to the data submission process an LEA uses to SFTP data to N-DEx. The LEA must have connectivity to N-DEx in order to use the batch submission process. The following provides step-by-step instructions for the LEA to adopt this method of data submission.

The batch submission process will start when an agency decides that they want to move their properly formatted data over to the N-DEx system via an SFTP process. Once the agency decides that they would like to send N-DEx data via this mechanism, and connectivity has been established to the N-DEx system, the following steps must occur.

- 1. The liaison emails the agency's data administrator instructions on how to create public / private keys for connection to the N-DEx SFTP servers. The basic information is as follows.
 - a. If the agency uses Unix or Linux
 - i. Open the command prompt on the data submission server and type the following

- ii. `ssh-keygen -t rsa -b 2048`
- b. If the agency uses Windows
 - i. Utilize putty to generate a public private key pair

Note: The keys generated are specific to an individual data submission server. If more than one server is going to be submitting data, a key will need to be generated and exchanged for that server.
- 2. The agency must send the public key that was generated from the above step to the liaison using a secure method (ex. LEO email). The filename will be [LEA Name]_rsa.pub.
- 3. The N-DEx liaison gives the public key to the N-DEx system administrator for installation onto the N-DEx SFTP servers.
- 4. The N-DEx system administrator provides the login credentials for that agency to the liaison.
- 5. The liaison gives the LEA data administrator the login credentials for the N-DEx SFTP servers.
- 6. The LEA data administrator verifies connectivity by executing the following command.
 - a. `sftp username@153.31.167.7`
- 7. The LEA data administrator verifies that their files adhere to the N-DEx file size specifications.
- 8. The LEA data administrator then executes the following command:
 - a. `Put <filename>`
- 9. The LEA data administrator then looks into the directory where the file has been put to verify the existence of the file that has just been copied.
- 10. The LEA data administrator then has to terminate the SFTP session

3.6.3 Web Services Submission Process

N-DEx offers a submissions web service for those submitting agencies that wish to have their system send single documents to N-DEx on a more frequent basis. In order to submit data in this fashion the partnering agency will have to create a web services client, generate X.509 keys for authentication, and invoke the N-DEx ingest web service. The following paragraphs will discuss each of these steps in more detail.

The first step in submitting data via the ingest web services is to create a web service client for the ingest web service. To create the client, the submitting agency will be sent the Web Services Description Language (WSDL) file from the Operational N-DEx system. This WSDL will be sent to the LEA via email or shipped on CD to the LEA. The LEA will then create a web services client based off of the information in the WSDL.

After the web service client has been created, the LEA will also have to create an X.509 certificate to allow the LEA's data submission server to communicate with the N-DEx ingest server. Once the X.509 certificate is created, the LEA will be required to provide N-DEx the public key. N-DEx technical staff will aid the LEA in creating the X.509 certificate as necessary.

Once the LEA has created the client and certificate, data submission via web services can occur.

- Execute a web browser application
- Type <https://153.31.167.6/wsdl> in the web browser address area
- Accept the certificate into your web browser
- Accept the X.509 exchange between the LEA server and N-DEx
- Submit data via the Web Service

For N-DEx Increment 1 implementation, downtime is scheduled between the hours of 8pm and 10pm Eastern Standard Time. During this time the system will not be available for data submissions via web services.

3.6.4 Incident Submission via N-DEx Portal

Some agencies with a respectively lower number of incident reports may wish to log into N-DEx and type incident information into an online form provided by the N-DEx portal. Detailed information regarding data submission via the N-DEx portal can be found in the N-DEx users manual.

4 Initial Legacy Data Submission

N-DEx is gathering five years of historical data from partnering agencies in order to correlate and resolve information from incident reports in this timeframe. Due to its large nature, your initial dataset should be loaded onto an external media device (CD, DVD, external hard drive, or thumb drive) for manual submission to N-DEx. The external media device should be sent via Federal Express to your N-DEx liaison specialist.

Once your initial legacy data set has been ingested into the N-DEx system, routine data submissions can be sent to N-DEx via electronic transfer.