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

Law Enforcement
National Data Exchange

Concept of Operations

Version 1.5

Document Number: N-DEx-DOC-01125-1.5

Document Date: May 1, 2006

Record of Changes		
Date	**Description**	**Revision**
01/26/2006	Initial Draft version.	v1.0
02/02/2006	Updated full ConOps based on CJIS Executive Management and Department of Justice Office of Chief Information Officer review.	V1.1
02/17/2006	Updated full ConOps based on ConOps Task Force review. Submitted to CJIS APB Working Groups for review.	v1.2
03/31/2006	Updated full ConOps based on internal N-DEx Program Office review, Department of Justice Office of Chief Information Officer review, as well as CJIS APB Working Groups review.	v1.3
04/10/2006	Updated full ConOps based on CJIS Contract Administration Office, CJIS Executive Management, as well as FBI and Department of Justice Offices of Chief Information Officer final review. Submitted to CJIS APB Information Sharing Subcommittee.	V1.4
05/01/2006	Updated full ConOps based on internal N-DEx Program Office review, Department of Justice Office of Chief Information Officer review, as well as CJIS APB Information Sharing Subcommittee.	V1.5

1 Preface

The purpose of this document is to describe the Law Enforcement National Data Exchange (N-DEx) from an operational perspective. The intent is to inform the Performance-Based Procurement process selected for designing and building N-DEx and ensure that users and stakeholders both understand and share the N-DEx vision.

The term Concept of Operations (ConOps) is defined to include scenarios that illustrate N-DEx capabilities and services, options for integration with user systems and user access, system technical characteristics and requirements, assumptions about what is included in N-DEx, and an overview of the N-DEx implementation approach.

Sections 2 through 6 address N-DEx functional issues while Sections 7 through 11 describe technical matters.

In summary, the ConOps describes the "what" of N-DEx. N-DEx managers and the selected solution provider will address the "how of N-DEx," including issues such as a development timeline, governance, funding, requirements development, and other issues in a separate program management plan and associated design documents. This ConOps is to be used in conjunction with these other program documents to design and develop the system.

2 N-DEx Overview

The purpose of this section is to provide a broad overview of N-DEx and to serve as a conceptual framework for understanding the sections that follow.

2.1 N-DEx Vision

The vision of N-DEx is to share complete, accurate, timely and useful criminal justice information across jurisdictional boundaries and to provide new investigative tools that enhance the Nation's ability to fight crime and terrorism.

2.2 What is N-DEx and What Are Its Benefits?

N-DEx will provide law enforcement agencies (LEAs) with a powerful new investigative tool to search, link, analyze and share criminal justice information (e.g., incident and case reports) on a national basis to a degree never before possible. N-DEx will primarily benefit local law enforcement in their role as the first line of defense against crime and terrorism.

N-DEx will allow participating LEAs to detect relationships between people, places, things and crime characteristics, link information across jurisdictions and allow them to "connect the dots" between data that are not apparently related without information overload. This capability will occur primarily in the realm of structured data but can also include unstructured data. In addition, it will provide contact information and collaboration tools for LEAs that are working on cases of mutual interest.

Management of data shared in N-DEx will remain with the LEA that provided it. N-DEx will supply controls to allow LEAs to decide what data to share, who can access it and under what circumstances. It will allow agencies to participate in accordance with applicable laws and policies governing dissemination and privacy.

Although law enforcement will be the primary focus of N-DEx, future iterations will incorporate the full criminal justice community. The ultimate goal is to transform all criminal justice data into knowledge for the entire justice community.

2.3 How Can LEAs Participate in N-DEx and How will it be Funded?

N-DEx will offer a range of options to allow broad participation; ranging the spectrum from LEAs with automated records management systems (RMS) to those having paper-based systems.

To mitigate LEAs' costs and impacts, N-DEx will use nationally-developed standards and existing systems and networks. It also will help agencies get started by providing implementation support, tools and training. In addition, N-DEx managers will work with the Department of Justice (DOJ) to ensure existing grants/programs funds are made available to help mitigate implementation costs to participating agencies. Under the current budget environment, neither the Criminal Justice Information Services (CJIS) Division nor DOJ can guarantee this funding. However, ultimate success of the program will require a positive resolution to the funding issue.

The success of N-DEx will also require resolution of major governance, policy, technology and funding challenges. In response to these challenges, N-DEx will be built and deployed incrementally, reducing risk and providing benefit along the development path.

2.4 Guiding Principles/Assumptions

The value of N-DEx will extend beyond the power of technology to incorporate and implement a set of guiding principles developed in cooperation with local, state, tribal, and federal law enforcement. The following guiding principles and assumptions were considered in the development of this document:

2.4.1 The Key Success Factor

The N-DEx ConOps was developed in close collaboration with the local, state, tribal and federal LEAs that will be critical to the success of the project. Ensuring that N-DEx meets the real-world needs of law enforcement has been identified as the key success factor from the very beginning and will continue to guide the program throughout implementation and operation.

2.4.2 A Concept of Operations

The N-DEx ConOps is intended to be a document that describes the "what" of N-DEx; not "how" N-DEx is to perform functions to assist law enforcement in preventing and investigating crimes. As such, the ConOps is not a requirements document, but should be used with other N-DEx programmatic documents to assist in the design and development of the proposed N-DEx system.

2.4.3 Incremental Deployment

This document addresses N-DEx in its "end state" relative to the services and capabilities that will be implemented, as well as its users and data. However, N-DEx will be developed and deployed incrementally and many of the capabilities, data sources and uses described in this document will be implemented over time. The initial focus is on providing the more basic, but powerful capabilities associated with integrating disparate systems of incident and investigative data and providing tools for searching and sharing this law enforcement information. It is also important to note that the first deployment of the N-DEx System must provide successes that provide maximum value and ensure continued participation, as well as foster a growth in desire to participate in N-DEx by local, state, tribal and federal LEAs. The incremental deployment plan is summarized in Section 10.

2.4.4 Data Source Availability/Participation

The effectiveness of N-DEx is dependent upon widespread participation of organizations sharing their data. The availability and resources of data sources are beyond the control of the N-DEx Program.

2.4.5 N-DEx – Not a Statistical Reporting System

N-DEx is an information sharing system and is not intended to be used for crime statistics reporting. As such, N-DEx and the Uniform Crime Reporting (UCR) Program are considered to be separate programs. Participation in the National Incident-Based Reporting System (NIBRS) will not be a requirement for participating LEAs. However, N-DEx will use the standardization provided by NIBRS data elements to describe portions of the incidents and will add value to those agencies that participate in NIBRS. An LEA may report NIBRS through N-DEx, if they so choose. However, an LEA will not need to change the method of UCR/NIBRS reporting to participate in N-DEx.

2.4.6 N-DEx has Intelligence Value – Not an Intelligence System

N-DEx is not an intelligence system and will not contain intelligence data. Similar to other criminal justice systems (National Crime Information Center [NCIC], et.al.), the N-DEx information and tools will provide value to the intelligence community.

2.4.7 Management of Data

The management of LEA data shared in N-DEx will remain with the LEA that provided it. N-DEx will supply controls to allow LEAs to decide what data to share, who can access it and under what circumstances. It will allow agencies to participate in accordance with applicable laws and policies governing dissemination and privacy.

2.4.8 Role of the State Programs in N-DEx

The FBI CJIS Division has worked closely with state CJIS Systems Officers (CSOs) in the development and implementation of many of the CJIS systems that are replicated or provide service to the local, state, tribal and federal LEAs. Reasons that the FBI CJIS Division has worked through the CSOs are many. One reason is that this mechanism creates a central (single) point of contact for many CJIS related matters and responsibility/accountability for access and use of CJIS systems. A second reason is the varied landscape in the U.S. regarding laws and statutes relative to the operation of these systems, as well as the varied system types that connect and interact with CJIS Systems. Because of this varied landscape, the preferred method for N-DEx connectivity with systems that will provide data to N-DEx would be through this central CSO point within each of the 50 States. However, this may not be feasible in the short term, as the capabilities of many state programs are also varied; many are not ready to receive or transport data to N-DEx for information sharing purposes. Because of the variations among the systems and RMSs within the LEAs nationally, the N-DEx Program may be required to accept data or interface with user systems under a wider (less centralized) approach, which would also include Fusion Centers and regional information sharing efforts that fall outside of the auspices of the CSOs. Connectivity with any of the various systems will need to be coordinated and communicated through the CSOs to ensure compliance with applicable local and state laws and regulations as well as ensuring the migration of the state systems to become the primary conduits for N-DEx connectivity.

2.4.9 N-DEx Integration/Interfaces

An objective of the N-DEx implementation is to reduce the points of integration from a data and functionality perspective. Numerous regional information sharing efforts in place today have already integrated data from regional, state and local agencies. It is much more practical for these "repositories" to supply data to N-DEx on behalf of the local agencies, than for each local agency to implement N-DEx-specific data source interfaces. This concept of federating the N-DEx data paths (e.g., locals to regions, regions to states and states to N-DEx) facilitates N-DEx. Ideally, N-DEx would obtain its data from the 50 States' repositories working on behalf of the agencies within their states. This will reduce the points of integration from a data and functionality perspective, but will also minimize the system/user administration responsibility at the CJIS level and delegate this function to the agency in the best position to perform these functions (e.g., administer users, configure systems, determine roles for individuals). However, this model of aggregation is not occurring nationwide. As such, N-DEx must be able to obtain its data through a variety of options as permitted by policy. Some LEAs will provide their data directly to N-DEx and others will provide it to repositories that will in-turn provide it to N-DEx.

2.4.10 Integration/Implementation Flexibility

To encourage broad participation, N-DEx will offer a range of options for LEAs to integrate their current RMSs with N-DEx, ranging the spectrum from LEAs with automated RMSs to those having paper-based systems. In order for the success of N-DEx to occur, the architecture and development of the proposed N-DEx System must consider and incorporate the multiplicity of the potential local, state, tribal and federal RMSs that will provide data to N-DEx. As this landscape is varied, N-DEx will use nationally-developed standards and existing systems and networks to mitigate LEA costs and impacts, but a recognition of this varied landscape will be critical for N-DEx development.

In conjunction with integration, the N-DEx Program will develop a well-defined, thoroughly documented, and widely distributed project and program plan in conjunction with a clearly identified migration path throughout all N-DEx implementation phases. N-DEx will allow LEAs the flexibility to plan their own entry point and local implementation timelines. In addition, CJIS will deploy N-DEx capabilities in incremental stages. The N-DEx strategy is to divide implementation into sub-projects that can be developed independently with overlapping or concurrent timelines, including prototype projects to add incremental value along the development life-cycle.

2.4.11 Leverage Existing Standards, Systems and Networks

Many potential N-DEx participants are already members of some other trusted information sharing community (state, regional, federal, etc.). These users usually access and provide information through local mechanisms and sanctioned business processes. N-DEx will provide well-defined integration points allowing for inclusion of existing groups, technologies, locally vetted identities and policies into its broader information sharing architecture (i.e., CJIS systems, Regional Data Exchange [R-DEx], other DOJ components, and other federal LEAs). It is critical that existing infrastructures and systems be leveraged wherever feasible to reduce costs.

Recognizing that a tremendous amount of data standardization work has occurred (and continues to date), N-DEx must take advantage of this work and standards. Data standardizations include the work of Global, the Global Justice Extensible Mark-Up Language Data Model (GJXDM), the National Information Exchange Model (NIEM), the Law Enforcement Information Sharing Program (LEISP) Exchange Specification (LEXS) based on the latest NIEM release, et.al.

2.4.12 Organizational Accountability

An essential element for successful inter-agency cooperation is organizational accountability. A Memorandum of Understanding (MOU)/User Agreement will be the mechanism N-DEx will use to document what has been agreed upon with its information-sharing partners, including standards and controls that address access to each partner's data. A standard MOU/User Agreement will be employed but it will be augmented to address unique relationships with data providers.

2.4.13 Collaborative Development

N-DEx will be designed and built in consultation with its local, state, tribal and other federal partners in a collaborative manner. It will incorporate common policies, procedures, practices, capabilities, support services and connectivity architecture that will be necessary to allow N-DEx's law enforcement partners to access and use N-DEx information and to share their information. N-DEx cannot dictate these foundational sharing elements; they must be developed in a collaborative manner.

2.4.14 Classification

Only data classified as Sensitive but Unclassified (SBU) or below will be permitted within N-DEx.

3 Current Information Sharing Environment

The purpose of this section is to describe the current LEA information sharing environment, including current capabilities and challenges.

3.1 Current Systems

Nationally, powerful information sharing capabilities currently exist to support law enforcement. These systems provide critical services such as the identification of potential terrorists and fugitives, the discovery of criminal subjects' identities using fingerprint data, a national repository of criminal history records and other important capabilities.

Among the current capabilities upon which N-DEx will draw is the Federal Bureau of Investigation (FBI)'s CJIS Division systems, including NCIC, the Integrated Automated Fingerprint Identification System (IAFIS) and the Interstate Identification Index (III). (See Appendix B for a description of all CJIS systems).

- NCIC connects virtually all LEAs in the country and processes more than 4.5 million transactions per day in its mission to identify terrorists, apprehend fugitives, locate missing persons and recover stolen property.

- IAFIS processes more than 55,000 fingerprint submissions a day against a national fingerprint repository of approximately 51 million records. The system responds to inquiries from LEAs within minutes, allowing police all across the Nation to identify criminal suspects from their fingerprints.

- Once a suspect is identified through NCIC and IAFIS, users can access III to request a suspect's associated criminal history, including name, birth date, race, sex, aliases, etc.

Although local law enforcement broadly participates in and uses these national systems, the information they contain is largely status-based and passive (i.e., whether a person is wanted or on a watch list or has a fingerprint on file) or is historical in nature (i.e., information on a person's criminal record) and are not integrated nationally. In response to this issue, many states have recognized the need to share additional information across jurisdictional boundaries and have implemented state-wide programs to accomplish this information sharing. Also, regions have combined forces to develop regional initiatives to share incident information. However, these states and regions are not integrated at the national level. The primary target for N-DEx integration is the incident data of more than 18,000 LEAs that make up the front line of the Nation's defense against crime and terrorism.

3.2 Challenges

In spite of the national information sharing successes described above, some of the highest value law enforcement information is contained in incident data from criminal events and investigations. This information is located in the systems and records of individual LEAs, states and regional systems and is not being shared on a national basis.

In recent years, regional information sharing initiatives have demonstrated the value of this incident information for special purposes (e.g., task forces on drugs, gangs, organized crime, fraud). These models, however, were not intended to be physically scalable on a national level. As such, they are also not readily conducive to the creation of a national information sharing environment, although they would play an integral role in providing information to N-DEx.

In addition to the above, the challenges facing law enforcement have also evolved. Today's information challenges include:

- **Increasing Sophistication and Complexity of Crime and Terrorism:**
  Criminal and terrorist organizations have become increasingly complex. They are more sophisticated, mobile and networked, while law enforcement has remained stove-piped and relatively disconnected. This evolving complexity obscures relationships and activities, inhibiting the ability of law enforcement to obtain the information needed to link facts and discover patterns to more effectively combat criminal activity and terrorism.

- **Highly Fragmented and Autonomous Nature of Law Enforcement:**
  Law enforcement in the U.S. is organized into more than 18,000 separate local, state, tribal and federal jurisdictions, with independent governance, information systems and activities, and subject to their own set of circumstances, concerns and limitations. The multiplicity of jurisdictions and their autonomous nature engender inconsistent policies, practices and systems, and make coordination among agencies difficult.

- **Inadequate Information Sharing Standards and Policies:**
  Another result of the multiplicity of independent agencies is a lack of common standards and policies for information exchange. Despite efforts to coordinate and integrate, law enforcement information systems have been developed without the benefit of an overarching national information sharing strategy. Existing information technology systems were designed on a mostly ad hoc basis to address needs and exigencies of the time and were not built to exchange information across agencies. As a result, law enforcement information systems remain stove-piped, with limited interoperability and connectivity, inadequate for effective information sharing of the kind and magnitude needed today.

- **Complexity of Identifying Who Has the Right Information and How to Get It:**
  As a result of the fragmented nature of law enforcement and law enforcement information systems, the ability of police officers to discover helpful information that exists within the RMSs of the thousands of LEAs across the Nation is non-existent. Another problem is the lack of a national directory of LEAs and law enforcement personnel for finding out who to contact for questions.

- **Lack of access to complete, accurate and timely information:**
  Any single LEA's ability to "search" for information often is severely limited because many systems are manually updated, subject to varying business practices, separate data entry processes, and contain incomplete information. In addition, many local law enforcement records are still maintained on paper or, if electronic, are not stored in sharable formats for discovery. The inability of law enforcement to discover links between seemingly unrelated information is a key deficiency. Even if all systems and

data were connected, it is impossible to manually traverse millions of records to discover complex relationships and connections.

- **Current threats demand proactive capability:**
  Most current information sources are passive in that they require law enforcement to "know" something and "search" for something specific related to an event, incident or need. Many law enforcement cases involve partial evidence or facts (vehicle or suspect descriptions, property, weapons, etc.) that may represent "investigative interest." However, these items are often not searchable, and there is no method to communicate that interest among LEAs nationally. Crime prevention programs typically seek to target crime types, specific neighborhoods, or criminal demographics. Crime analysis, mapping, and prediction can assist in proactively deploying programs, resources, and manpower where it is most needed and where it can best impact crime before it happens. Most agencies lack the comprehensive data for modeling and cannot afford these sophisticated technologies.

- **Cumbersome, ineffective and disconnected law enforcement community collaboration:**
  As a result of inconsistent policies and practices, those who do share sensitive information cannot always be sure how it will be used, that it will be protected, or who will ultimately have access to it. These legitimate concerns can make agencies reluctant to share their information and unwilling to participate fully in information sharing initiatives. This legacy has undermined previous information sharing efforts and now constitutes one of the most intractable barriers to improving information sharing. Also, many LEAs have mutual aid agreements for emergencies, but most do not know if neighboring LEAs have data or related cases that could assist them.

- **Enhance information sharing while ensuring privacy:**
  Ensuring privacy is essential, but complex since there are thousands of LEAs - each with its own privacy laws, policies and information gathering protocols. The maintenance and exchange of shareable information must comply with all applicable privacy standards and legal requirements. LEAs must insure and be assured the information they contribute does not violate their own standards or jeopardize their missions or their personnel.

4 N-DEx Values

This section describes the values that N-DEx will provide in addressing the challenges discussed above and the principles that will guide its design and implementation.

4.1 Values Summary

N-DEx will provide measurable value by systematically confronting the challenges of law enforcement information sharing identified in Section 3.

Figure 4-1: N-DEx Values

N-DEx Values	Information Sharing Challenges
A national system for the integration and discovery of criminal justice information	Lack of access to complete, accurate and timely information. Highly fragmented and autonomous nature of law enforcement.
An electronic catalog of structured criminal justice information that provides a "single point of discovery"	Complexity of identifying who has the right information and how to get it.
Leveraging technology to relate massive amounts of data into useful information	Inability to "connect the dots" and not be overwhelmed by data.
Automated discovery of patterns and linkages to detect and deter crime and terrorism	Increasing sophistication and complexity of crime and terrorism. Systems based on reactive information when current threats demand proactive capacity.
Nationwide, law enforcement communication and collaboration	Cumbersome, ineffective and disconnected law enforcement community collaboration.
Enhance sharing between sharing partners through technology and policy	Enhance information sharing while ensuring privacy. The need to ensure that control over data remains with the owner of the data and privacy is maintained.

A National System for the Integration and Discovery of Criminal Justice Information

N-DEx will create a national information sharing system, including functional capabilities, business processes, policies and technology standards to enable the sharing of data among LEAs throughout the United States. Key components include:

- Core functional capabilities, including a single point of "integration and discovery" for national law enforcement data, comprehensive search and analysis, a robust security and privacy model, a national user directory of LEAs and law enforcement personnel throughout the U.S., and community policies on the "roles, rights and privileges" for information sharing among law enforcement users.

- A flexible infrastructure and connectivity architecture that provides multiple options for LEAs to participate and integrate with N-DEx, including standards for establishing and operating local connectivity with N-DEx, ensuring security and automating business rules to maintain management rights over data submitted to N-DEx and leveraging existing standards and systems.

A Catalog of Criminal Justice Information that Provides a "Single Point of Discovery"

N-DEx will establish a common "index" or "catalog" of national criminal justice information containing data elements from LEAs' records nationwide. This thin layer of data about the who, what, when, where and how contained in records will serve as a repository for searches and analysis. Initially, users will log onto the N-DEx system as a point of discovery, but over time it is anticipated that N-DEx will be integrated seamlessly into LEAs' records management systems. This core component of N-DEx will allow:

- Automated and timely discovery and access to relevant data throughout the country.

- LEA control over the administration of its agency data to ensure the needs for data stewardship and meet respective local laws and policies for information dissemination.

- Policy-driven and automated methods for accessing, processing and disseminating data to protect contributing LEA data from unauthorized access and misuse.

Leveraging technology to relate massive amounts of data into useful information

N-DEx will deliver core capabilities for sorting, organizing and correlating the indexed data, including:

- Improve a user's ability to effectively manage the discovery of information by providing system search, automatic correlation (i.e., linking of related people, places and events), filters, links and associated files.

- Provide advanced search capabilities to discover information when there is a lack of key information for conducting a typical query search (i.e., a user doesn't know what he/she doesn't know), providing valuable insights into previously unknown incident data.

- Tools to allow law enforcement to analyze incident data to a degree never before possible.

- Automate information sharing and provide proactive support in the identification, processing and dissemination of information that should be shared, including automatic information services through subscriptions, notifications and alerts. These automated routines will help reduce or eliminate time-consuming manual processes, including watch list correlation and fraud identification.

Automated Discovery of Patterns and Linkages to Detect and Deter Crime and Terrorism

N-DEx will incorporate a suite of special purpose tools to increase the effectiveness of law enforcement functions (e.g., tactical, strategic, operational and administrative functions). These tools will provide:

- Automated data association and linkage analysis to enable multiple paths to discovering related data, incidents, people or events. This extended view into the relationships between data sources will provide valuable material for case processing, investigation and prosecution.
- The ability to traverse millions of disparate records by "scoring the index data" by degrees of "reliability" and "relevance" to search criteria. In this way, public safety and homeland security will be enhanced by increasing a local agency's ability to operate tactically with strategic information.

Nationwide, Instantaneous, Cross-Jurisdictional Communication and Collaboration

N-DEx will leverage its national connectivity environment to create a directory of all LEAs and LEA users to facilitate new methods of law enforcement collaboration. This ubiquitous common connectivity - coupled with standardized information, tools and capabilities—will enable many automated information sharing tasks and collaboration opportunities, including:

- A national nexus for bringing together the most important element of law enforcement: the men and women on the front lines of crime and terrorism deterrence and prosecution.
- Ability to contact, communicate and collaborate with law enforcement data owners relevant to cases, investigations or discovered data.
- On-the-fly creation of collaborative law enforcement teams or multi-jurisdictional investigations where team members can share secure information through "virtual" workspace, tools and communication capabilities.

Ensure Sharing Between Sharing Partners Through Technology and Policy

LEAs that contribute data to N-DEx will retain management of their data and retain control over who may access it and under what circumstances. The N-DEx governance authority will develop uniform policies to protect against misuse of information. These policies will include organizational accountability, including an audit function and the application of sanctions if a participating agency fails to meet its obligations on such policies as:

- Privacy: Privacy policies will be complex since N-DEx will collect sensitive data from thousands of LEAs—each with its own privacy laws and information gathering protocols. N-DEx must be developed to ensure that the maintenance and exchange of shareable information comply with applicable privacy standards and legal requirements. N-DEx participants must insure and be assured the information they contribute does not violate their own standards or jeopardize their missions or personnel. The originators of data and information will retain management of their data. LEAs will not be required to submit data that they do not wish to share. Through technology and policy, N-DEx will provide an enhanced degree of privacy and cooperation among the participating law enforcement community beyond what is common practice today.

- Memoranda of Understanding/User Agreements: The rules, roles, practices, procedures and responsibilities to which each partner is committed will be formalized through the mutual development of MOUs/User Agreements. In consultation with N-DEx stakeholders, standard templates will be developed for the MOUs/User Agreements in order to normalize format and content requirements. These agreements will be customized as necessary and executed with participating agencies and regional information sharing partners.

- Management, entry and maintenance of information: To ensure that management of information made available for sharing remains with the organization that originated the data and that such data cannot be distributed to others without the permission of the owner.

- Quality Assurance/Quality Control: To establish the data quality responsibilities for accuracy, completeness, and timeliness of shared data. Additionally, while no core or minimum data set will be required for participation with N-DEx, participating LEAS are encouraged to submit as many N-DEx data elements as they have available.

- Auditing: To establish an audit capability and associated sanctions for non-compliance with mutually agreed upon policies.

- Security: Identify the common security controls partners are responsible for implementing and maintaining.

- Authorization/Authentication: To identify the responsibilities each partner has for authenticating the identity of LEA users and authorizing information shared under MOUs/User Agreements.

- Technical Standards: To guide each partner in its interoperability with N-DEx.

- Training: To establish partner responsibilities for training their employees who access information obtained under the MOUs/User Agreements.

- Metadata Ownership: To establish that the FBI CJIS Division is the owner of any metadata that is created as a result of data submitted by N-DEx participants. N-DEx capabilities will be developed through system design and development to track the creation and maintenance of said metadata and information pertaining to the metadata. If applicable, these capabilities will conform to laws and regulations relative to the maintenance of records (e.g., System of Record Notification, Privacy Act). (See Section 9.7 for further discussion.)

5 N-DEx Services and Capabilities

This section describes the N-DEx services and capabilities and their value to law enforcement in terms of their ability to discover useful information within millions of records that will be shared through the system.

Like the data aggregated in N-DEx, these services and capabilities are not new to law enforcement. But in today's environment, they are not uniformly available. In addition, current data is fragmented and often hidden in insular stovepipes. Both of these problems prevent vital information from reaching those that need it in a timely fashion. N-DEx will address these challenges by providing services and capabilities on a national scale.

5.1 N-DEx Information Services

N-DEx information services represent "under the hood" functionalities which benefit users but are not directly visible to users. These services are used by N-DEx capabilities to provide useful outcomes. The services collect and transform raw contributor data into information that can be easily shared, searched and queried to support investigations and analyses, including:

- Entity and Relationship Service
- Incident/Case Correlation Service
- Automated Processing Service

5.1.1 Entity and Relationship Service

The primary purpose of this service is to consolidate and merge records and/or data that relate to the same entity (e.g., a person, vehicle, address) and add additional information that will further help link and inter-relate other entities and incidents. It also will serve to provide effective results on user queries, even in cases where there is not an exact, literal match. If N-DEx only recognized entities as matching when they matched exactly, a large percentage of connections would be missed, reducing the effectiveness of N-DEx. The entity and relationship service will include the following:

- Entity Resolution: Automatically determine related entries that may contain varying or non-exact details. For example, "JT Smith" and "Jimmy Smith" are determined to have enough similar identifying information that there is a high probability that they are the same person. N-DEx will, at a minimum, identify potential candidates for consolidation. Other capabilities to be considered include the ability for a user to manually consolidate entities (i.e., a determination has been made by a user that the two entities are actually the same) and automatic consolidation of entities based on thresholds.

- Entity Correlation: Identifying relationships among entities even if they are not obvious or not specifically identified as related in any one record. Additionally, entity correlation will create and manage linkages to source records. For example, a Charleston Police Department incident report shows an address of 123 Main Street for Jim Smith and a separate Charleston incident report shows Bob Woods with an address of 789 Main Street. However, a Columbia Police Department booking report shows Woods recently claimed an address of 123 Main Street, Charleston, indicating a possible correlation between Smith and Woods.

5.1.2 Incident/Case Correlation Services

This service is similar to Entity Correlation but focuses on the "patterns" that link incidents/cases. These patterns include crime characteristics or modus operandi, criminal characteristics or criminal signatures that could link incidents and ultimately suspects to serial crimes. This service will automate the current manual and time intensive practice of searching through incident reports for similarities and help associate records that do not contain exact matches.

5.1.3 Automated Processing Service

Automatically performs processing upon submission of data to the system and provides notifications/alerts to users for items that may be of interest to them. The processing performed will be based on expert knowledge, standard procedures and best practices of law enforcement. For example, N-DEx will check all new suspects entered into the system against terrorist watch lists or notify/alert users of addresses that are known to be associated with other suspected terrorists. Another example, all person entities contained in submitted incident reports are checked against parole records for possible parole violations. Determinations for sending notifications/alerts to points of contact (POCs) will be based on rules or exceed "thresholds" of relevancy such that users will not be overwhelmed with meaningless notifications/alerts.

5.2 N-DEx Capabilities

User-driven capabilities consist of the applications that users can deploy to benefit from the vast amounts of information to be contained in the system, including:

- Search
- Subscription
- Notification
- Visualization
- Analytical
- Reporting
- Collaboration

Section 6 contains scenarios which describes each of the following capabilities within the context of case and investigation examples.

5.2.1 Search

The Search capability will be N-DEx's most prominent user-visible capability. It will be designed to support the needs of a diverse user base with varied computer skill levels to search and discover information for tactical, strategic, operational and administrative law enforcement purposes.

N-DEx users will have the capability to search for specific entities (people, places or things), crime characteristics, perform key word searches and find records (e.g., incident/arrest report). Users will also have the capability to determine "who else is looking, or has looked for" the same entities or items of mutual interest. As indicated previously, searches will return the output from Entity & Relationship services. This will allow users to discover and “drill down” through other related records and data to further the analysis of an investigation. Search capabilities will include both basic and advanced search functions. The basic search will be available through a simple user interface requiring very little training, while more experienced users can deploy advanced searching (e.g., using Boolean, wildcard operators).

In addition, the N-DEx search capability will provide extensive support for searching where the results are tuned to a user-defined business need (homicide investigators, narcotics investigators, crime analysts, et.al.). This capability, through filtering and ranking of results, will mitigate the problem of being overwhelmed by data.

5.2.2 Subscription

Subscription capability will allow law enforcement personnel to register for future information about entities and subjects of interest and their searches. Users will be able to establish subscriptions based on existing entities in the system and ask to be notified of updates and/or changes to the status or the availability of additional information on the entity. Also, they will be able to register for notification of future information about entities that are not known to N-DEx to include "who else is/was looking" for similar entities of items of interest. This capability will provide a key foundation for supporting case de-confliction and encourage potential case collaboration.

5.2.3 Notification

Notification capability will provide a means for N-DEx to automatically deliver specific messages to specific users or groups of users.

Under certain circumstances, N-DEx will generate notification/alert messages which need to be delivered to a specific user, even if the user is not currently logged in to N-DEx. For example:

- Data are sent to N-DEx which matches a subscription request previously registered by the user.
- The user is the POC on a record marked for Restricted Access, and another user’s search request matches data contained in the record.
- Automated processing will produce various messages based on correlations and applied business rules.

Notification/alert messages will have an associated priority. Users can configure the manner in which specific types and/or priority of notification messages should be delivered. A user or group of users may determine which notification/alert messages they or their agency wish to receive within guidelines set forth by policy. Other types of notification/alert messages may be globally defined such that a user or group of users will be unable to opt out of receiving the notification. Possible means of delivery include:

- Message displayed when user next logs into N-DEx
- E-mail
- Page or text message/Short Messaging Service (SMS)
- Message passed to user's local system (e.g., local RMS)
- Instant messaging

5.2.4 Visualization

Visualization capability will provide visualization tools to make it easier to use and understand the “knowledge” behind the vast amount of information in the system and the complex results from correlation, search, and report functions. These tools will provide both tabular and graphical representations of data to allow navigation through relationships, trends, and timelines of crimes and activities as the user sees fit. It also will have the capability to overlay data on geographic maps with various views of the data. With these tools, users can "drill down" into detailed data or navigate through complex relationship networks and view the data in a variety of representations for effective analysis. For example, a user's search request may hit on entities contained in numerous records. If the result information looks relevant to the user, he may choose to view the entire record.

5.2.5 Analytical/Reporting

Analytical/Reporting capability gives administrators, analysts and investigators the ability to generate reports from N-DEx data for investigative analysis, distribution and sharing. It will allow N-DEx to support law enforcement’s investigative reporting needs from a central platform. Through this capability, N-DEx will generate investigative online reports including graphic displays of data for use in predictive modeling, reporting, tracking and trending of crime for operational purposes but not for statistical crime reporting and publication. Analytical capabilities in conjunction with reporting will assist investigators and analysts in identifying areas for further investigation beyond what N-DEx provides through its automated processing service. These tools assist investigators and analysts in the identification of criminal networks, crime patterns, crime trends, and crime problems. For example, an analyst could use this capability to determine a “hot spot” of crime activity in a geographic region warranting further investigation. The investigator could then “drill down” into the underlying information forming the “hot spot” to determine the relationships among the entities involved in that information.

5.2.6 Collaboration

The N-DEx Collaboration capability will allow LEA users to electronically locate others working on similar cases and dynamically create investigative teams enabling real-time sharing of information that leverages the individual knowledge of police officers, analysts and investigators to a greater whole. This capability will be particularly important in the early stages of N-DEx implementation when data may be fragmented/incomplete or will not be as abundant as it will be in later stages where investigators can draw conclusions based on the returns of data.

Additionally, some of the underlying, “deeper” investigative information developed by the LE community will always exist outside of N-DEx (e.g., within the LEAs case files or knowledge held by investigators) and will not be included when the LEA generates data for an incident or investigation. In these instances, N-DEx will direct users performing a search or other query to contact information where they can pursue more information. For example, a response to a user’s search request may include a contact list of those who submitted data used in the search response. As another example, a user could create an online task force comprised of a group of users across jurisdictions to solve an important case. The investigative users could create “folders” or common spaces to share their analyses produced by N-DEx, create discussion forums about the case, and generally communicate among the group, while preventing sharing of this information outside of the group.

Per N-DEx policy, LEAs will determine the process for being contacted for collaboration purposes, whether through e-mail, telephone or other mechanism. Users will be able to further customize the method(s) selected by their respective LEA in how they prefer to be notified relative to both Notification and Collaboration capabilities.

6 Law Enforcement Scenarios

This section details scenarios to demonstrate the aforementioned proposed services and capabilities of N-DEx. Each scenario follows a similar format including a description of the situation and associated data input, the scenario outcome in terms of operational situation, potential system outputs and the conceptual N-DEx processing that made the outcome possible. These law enforcement scenarios demonstrate tactical, operational, strategic and administrative uses of N-DEx, the various services and capabilities discussed previously and are organized by services and capabilities.

The table below depicts the various scenarios and the services and capabilities that are employed to support a specific outcome. The table provides a cross reference between service/capability depicted by the scenarios and their law enforcement function.

Table 6-1. – Law Enforcement Scenarios Cross Reference

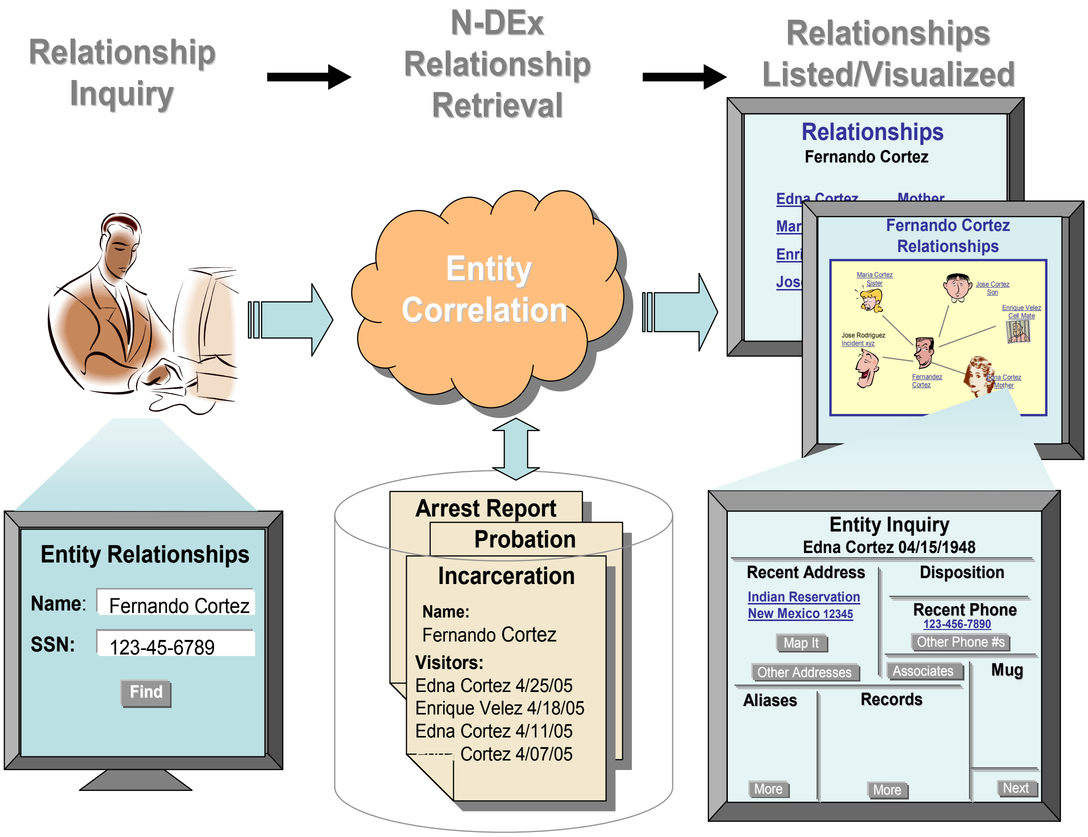
	Law Enforcement Functions			
Service/Capability	**Tactical**	**Operational**	**Strategic**	**Administrative**
Entity Resolution		4, 5	4	
Entity Correlation	15, 16	1, 2, 3, 7, 10, 15, 16		
Incident/Case Correlation		6, 17	6, 17	17
Automated Processing	8, 9, 22	4, 7, 8, 9, 22	4	
Search	11, 13, 14, 15, 16	1, 2, 3, 5, 10, 11, 12, 14, 15, 16, 20, 21		
Subscription	14	4, 14, 21	4	
Notification	6, 8	4, 6, 7, 8	4	
Visualization	11, 15, 16, 18	1, 2, 3, 11, 15, 16, 17, 18, 19	17, 18, 19	17, 18
Analytical/Reporting	18	17, 18, 19	17, 18, 19	17, 18
Collaboration	16, 18	2, 4, 6, 7, 16, 17, 18, 19	4, 6, 17, 18, 19	17, 18
Authorization and Security	22	20, 21, 22		

Note: The inclusion of sources of data (incident reports, arrest/booking information, incarceration, probation/parole, et.al.), specific user accesses (Police Officers, Probation Officers, Parole Agents, Analysts, et.al.), and data types (witness/victim information, et.al.) are used as an illustration of the breadth and scope of data that could potentially be available in N-DEx as well as users who could make use of the N-DEx system. Inclusion of data types beyond criminal incident reports and access to the system by the multiplicity of law enforcement users are policy issues to be vetted through the N-DEx governance process. The scenarios that follow should not be construed as an endorsement of any particular data or user type. The scenarios are also not intended to depict that N-DEx supersedes standard law enforcement procedures but how N-DEx may assist an investigator or an investigation. Finally, the user interface screens illustrated in the scenarios are for concept presentation only and do not imply a user interface design.

6.1 Entity Correlation

Scenario 1	**Entity Correlation (Tabular and Graphical)**
Capability	Entity Correlation; Search; Visualization (including "drill down")
Data	Arrest Reports; Probation Records; Incarceration Records
Crime	Money Laundering
Functional Areas	Operational
Scenario	Fernando Cortez fails to report for his voluntary surrender in Denver, Colorado, to begin a seven-year prison sentence for money laundering, and police enter an arrest warrant into NCIC. Officers search N-DEx for people connected to Cortez derived from the information contained in incident reports and other criminal justice reports previously entered into N-DEx. N-DEx finds the names, addresses and other identifiers of more than 100 associates of Cortez. The officers sort the results by those with the highest number of associations to Cortez and asks N-DEx to display the results on a map. Edna Cortez, the fugitive's mother who visited him every month of his incarceration, lives on the San Felipe Indian Reservation near Santa Fe, New Mexico.
Outcome	Officers in Denver contact San Felipe Indian Reservation tribal police who speak with Edna Cortez. They learn that she has been in contact with Fernando and agrees to make an effort to convince him to surrender.

N-DEx Process that Allows Outcome

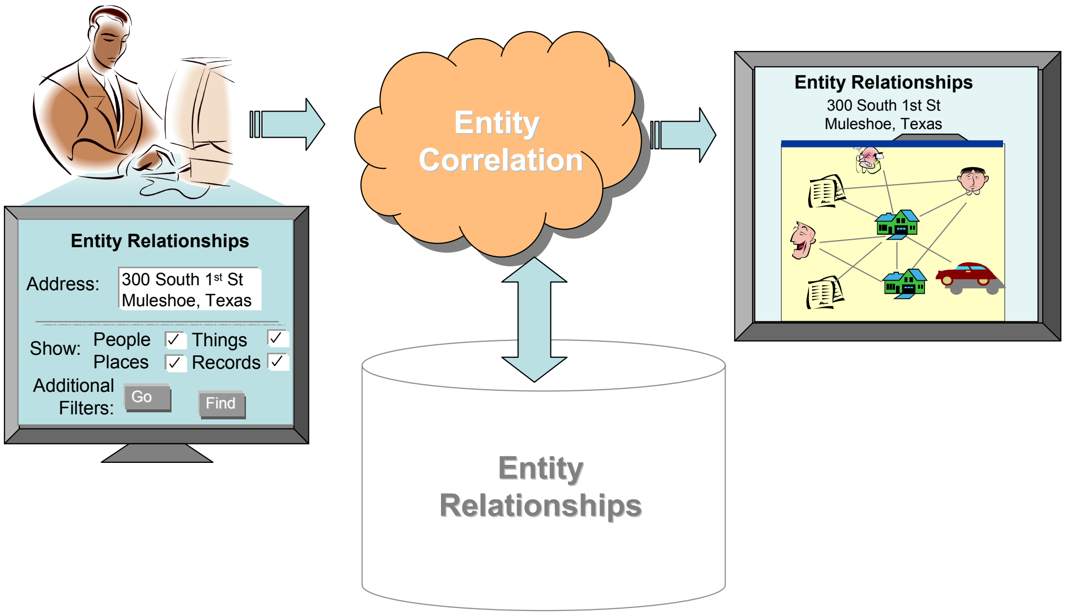


As depicted, N-DEx presents users with all known relatives and associates of a subject from all available records within N-DEx, including incident reports, arrest records, corrections records and parole records. (The integrated response can come from the information input into N-DEx as well as leveraging information available within systems such as NCIC, IAFIS, III, et.al.). N-DEx also provides a visualization of the relationships in a graphical representation that helps users analyze complex relationships and allows them to "drill down" to obtain specific information on persons of interest (in this case, the mother).

Scenario 2	Entity Correlation (Insurance Fraud)
Capability	Entity Correlation (Non-Obvious); Search; Visualization; Collaboration
Data	Incident Reports; Bureau of Immigration and Customs Enforcement Reports
Crime	Insurance Fraud
Functional Areas	Operational
Scenario	The National Insurance Crime Bureau (NICB) contacts the Texas Department of Public Safety (TDPS) about suspicious automobile insurance claims. NICB reports that member insurance companies paid out claims eight times over the past three months to members of one family at the same address (300 South First Street, Muleshoe, Texas). All claimed they were victims in two-car collisions. N-DEx identifies the address as being the address of Mike Sullivan, a victim in multiple police reports, including a burglary report, two stolen vehicle reports, and a pedestrian hit-and-run accident. Using N-DEx's search capability, the user finds similar victim reports involving another member of the family, Bob Sullivan, at different addresses in Oklahoma and Louisiana. Additionally, N-DEx identifies Immigration and Customs Enforcement (ICE) reports in which Bob Sullivan uses an address of 200 North Second Street, Muleshoe, Texas. N-DEx links this new address to multiple fraud investigations by the Bailey County Sheriff's Office (BCSO).
Outcome	As a result of the N-DEx ability to identify, correlate and share information between TDPS, NICB and BCSO, police were able to identify a second Sullivan family member involved in similar fraud in Oklahoma and Louisiana, which led to the opening of an investigation of the Sullivan family in three different states.

N-DEx Process that Allows Outcome

Record Search/ Find Associations → N-DEx Searches Records and Correlates Relationships → Relationships Identified Graphically


Entity Relationships

Address: 300 South 1st St Muleshoe, Texas

Show: People ✓ Things ✓ Places ✓ Records ✓

Additional Filters:

Entity Relationships

300 South 1st St

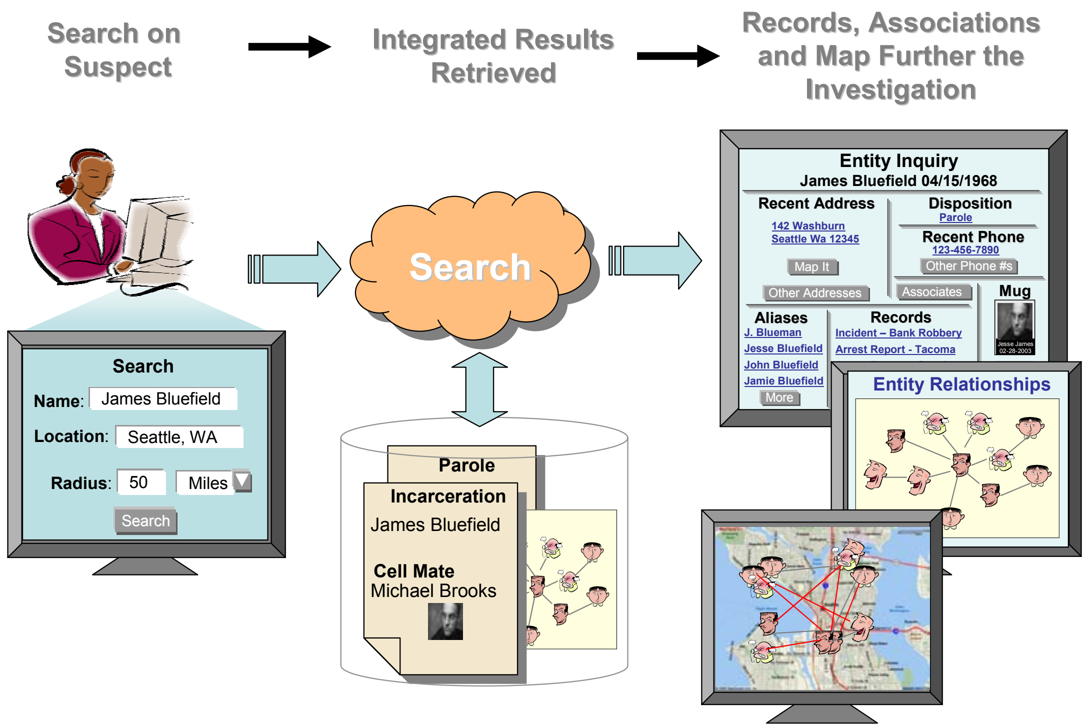
Muleshoe, Texas

As depicted, N-DEx allows the discovery of non-obvious relationships between people, locations, records, etc. In this case, the investigator finds people related to an address and other locations where the same people appear in various records.

29

Scenario 3	**Entity Correlation (Associates/Relationships)**
Capability	Entity Correlation; Search (Person); Visualization (Mug Shots, Geographic)
Data	Incarceration Records
Crime	Bank Robbery
Functional Areas	Operational
Scenario	An anonymous source telephones the FBI to identify a person responsible for a string of bank robberies in the Seattle, Washington area. Prior to this tip, the only fact known about the robber is that he worked with an accomplice because he always enters the passenger side of the getaway car. Because he was masked, the robber could not be identified and witnesses never had a clear view of the driver. The tipster identified the robber as James Bluefield. Investigators search N-DEx for Bluefield and find incarceration records on him from two previous prison sentences. The records identify his past cell mates. Investigators then use N-DEx to view the results geographically, associating Bluefield's ex-cell mates with the area where the robberies occurred. N-DEx identifies four ex-cell mates now living in the Seattle area. Two of the four former cell mates Michael Brooks and Tony Green, met Bluefield in prison while serving time for bank robbery. Investigators show mug shots of Brooks and Green to bank employees. One employee recognizes Brooks as a customer she assisted with a loan inquiry the day before the robbery.
Outcome	Based upon this information, agents begin surveillance on Brooks' residence and capture Bluefield when he shows up to visit Brooks. As a result of questioning both Brooks and Bluefield, police learn of another robbery being planned.

N-DEx Process that Allows Outcome



Search

Name: James Bluefield

Location: Seattle, WA

Radius: 50 Miles

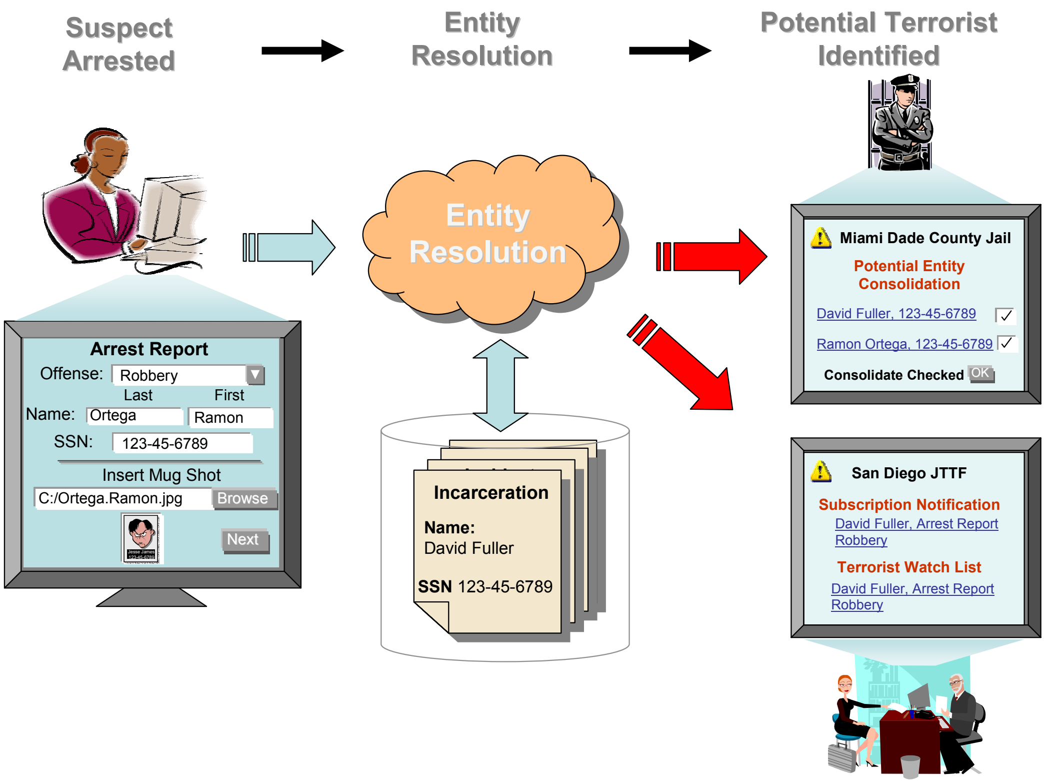
Search

The N-DEx Search capability provided the investigator with records on a suspect in a bank robbery. N-DEx takes advantage of previously submitted relationships (contained within a record) and identifies new relationships between entities (i.e. , people, places and things) using its Entity Resolution and Correlation capabilities as new records are processed when they are ingested. Subsequently, when records are searched, the user has access to all information on that entity (in this case, a person) and also has access to the relationships maintained within a record and relationships identified by N-DEx as it searches new records against all other records. In this case, the records contained related information on ex-cell mates as well as mug shots that helped further the investigation by providing additional information on one suspect and providing a link to another suspect.

6.2 Entity Resolution and Notification

Scenario 4	**Entity Resolution (False SSAN Leads to Terrorist)**
Capability	Entity Resolution; Automated Processing; Subscription; Collaboration; Notification
Data	Arrest/Booking and other records to support Entity Resolution
Crime	Terrorism
Functions	Operational; Strategic
Scenario	Miami police arrest Ramon Ortega for burglary. At the time of his booking and processing, police record biographical information and photographs. For identification, Ortega shows police a Social Security Card with the Social Security Account Number (SSAN) of 123-45-6789. The department sends Ortega's booking information to N-DEx as part of its daily batch submission. N-DEx automatically searches Ortega's identifying information (name, SSAN, etc) and identifies incident reports, indicating that Ortega may actually be David Fuller, an identified terrorism suspect believed to have illegally entered the U.S. Prior to this arrest, the San Diego Joint Terrorism Task Force (JTTF) had set a subscription for Fuller's name and SSAN in N-DEx. Based on this subscription and Fuller being on a Federal Terrorist Watch List, the San Diego JTTF receives an automatic notification of the Ortega arrest in Miami. In addition, N-DEx automatically alerts Miami police of the possibility that Ortega and Fuller are the same person. A member of the San Diego JTTF then contacts Miami authorities for further information about Ortega/Fuller. Miami police forward their information, including fingerprints and mug shots using e-mail. This allows San Diego to verify Fuller's true identity, resulting in a request that Miami hold Fuller for extradition to California.
Outcome	N-DEx capabilities collate disparate information from the Federal government and two police jurisdictions a continent apart and share the information; thereby, foiling an attempt by a terrorist involved with criminal activity to conceal his identity.

N-DEx Process that Allows Outcome



Arrest Report
Offense: Robbery
Name: Last: Ortega First: Ramon
SSN: 123-45-6789
Insert Mug Shot
C:/Ortega.Ramon.jpg Browse
Next

Incarceration
Name: David Fuller
SSN 123-45-6789

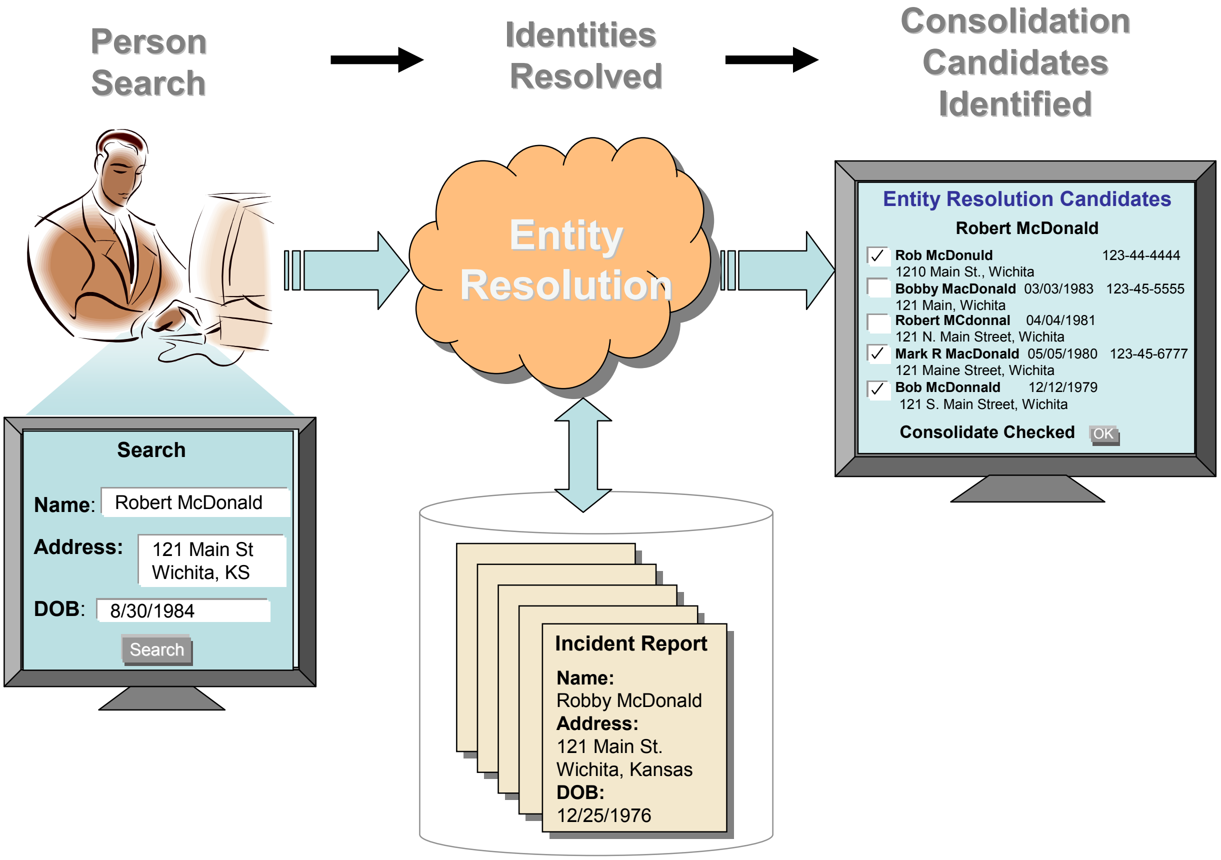
Miami Dade County Jail
Potential Entity Consolidation
David Fuller, 123-45-6789 ☑
Ramon Ortega, 123-45-6789 ☑
Consolidate Checked OK

San Diego JTTF
Subscription Notification
David Fuller, Arrest Report Robbery
Terrorist Watch List
David Fuller, Arrest Report Robbery

As depicted, N-DEx automatically performs Entity Resolution capabilities which results in a notification to Miami that Ortega may be using a false name (agencies involved would be notified only if they configured their individual notifications accordingly). N-DEx Automated Processing capabilities also correlate Fuller as a known terrorist. This results in an alert/notification to the terrorism task force that a known terrorist, using a false name, is involved as a suspect in a burglary in Miami.

<table>
<tr><th>Scenario 5</th><th>Name Resolution to Identify Robbery Suspect</th></tr>
<tr><td><b>Capability</b></td><td>Entity Resolution; Search</td></tr>
<tr><td><b>Data</b></td><td>Incident Report</td></tr>
<tr><td><b>Crime</b></td><td>Property</td></tr>
<tr><td><b>Functional Area</b></td><td>Operational</td></tr>
<tr><td><b>Scenario</b></td><td>Investigators with the Wichita, Kansas Police Department question Robert McDonald in a stolen property case. The investigators check NCIC and III but get no matches. They then perform an N-DEx search, but again find no matches with McDonald and the other identifiers provided by the suspect, including the address 121 Main St., Wichita, Kansas and an SSAN. However, N-DEx does identify five references to the Main Street address, linked to variations on the suspect's name as well as variations of his SSAN and date of birth.
<table>
<tr><th>Address</th><th>Name</th><th>DOB</th><th>SSN</th></tr>
<tr><td>121 Main St., Wichita</td><td>Rob McDonuld</td><td>01/01/1980</td><td>123-44-4444</td></tr>
<tr><td>121 Main, Kansas City</td><td>Bobby M. MacDonald</td><td></td><td>123-45-5555</td></tr>
<tr><td>121 North Main, Topeka</td><td>Robert McDonnal</td><td>12/12/1979</td><td></td></tr>
<tr><td>121 Maine St, Wichita</td><td>Mark R. MacDonald</td><td>01/01/1980</td><td>123-45-5555</td></tr>
<tr><td>121 S Main St, Wichita</td><td>Bob McDonnald</td><td>12/12/1979</td><td></td></tr>
</table></td></tr>
<tr><td><b>Outcome</b></td><td>N-DEx returns potential leads suggesting McDonald's involvement/participation in other incidents. After further analysis, investigators determine that McDonald is the same person in each incident, despite his use of false information.</td></tr>
</table>

N-DEx Process that Allows Outcome



Search

Name: Robert McDonald

Address: 121 Main St
Wichita, KS

DOB: 8/30/1984

Incident Report

Name:
Robby McDonald
Address:
121 Main St.
Wichita, Kansas
DOB:
12/25/1976

Entity Resolution Candidates

Robert McDonald

☑ **Rob McDonuld** 123-44-4444
1210 Main St., Wichita
☐ **Bobby MacDonald** 03/03/1983 123-45-5555
121 Main, Wichita
☐ **Robert MCdonnal** 04/04/1981
121 N. Main Street, Wichita
☑ **Mark R MacDonald** 05/05/1980 123-45-6777
121 Maine Street, Wichita
☑ **Bob McDonnald** 12/12/1979
121 S. Main Street, Wichita

Consolidate Checked

As depicted, N-DEx's Entity Resolution capability alerted the investigating officers of a consolidation of person entities. Based on the information (names, address, phone number, etc.) about a person in multiple records, N-DEx correlated the data, resulting in the identification of candidates for consolidation. In this case, the N-DEx user decided that indeed three of the potential candidates for consolidation presented by N-DEx have a very high likelihood of being the same person.

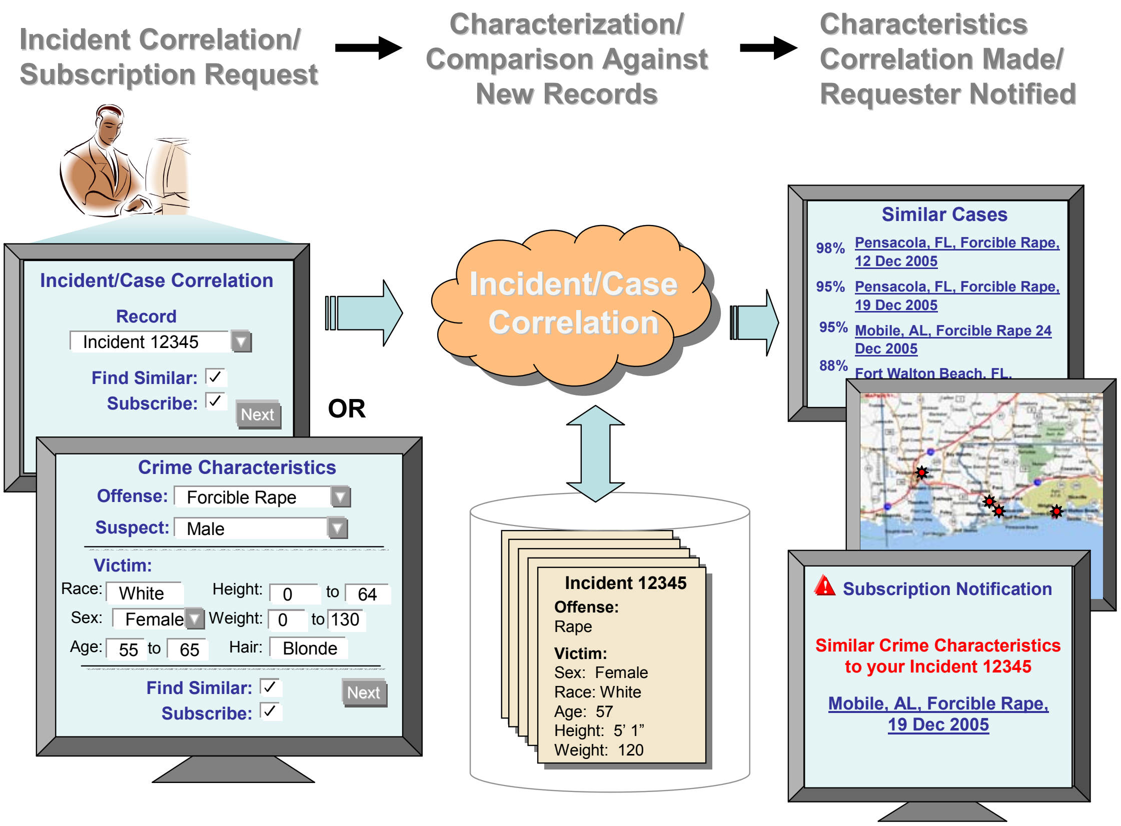
It should be noted that this scenario is intended to show two functions of N-DEx. First, that N-DEx performs entity resolution and identifies possible candidates for consolidation. Second, that N-DEx doesn't necessarily automatically consolidate entities, but presents this information to the user for consolidation. This is similar to the process used for fingerprint consolidation. The details of how this would function and how it would be presented to the user needs further analysis.

8

6.3 Incident/Case Correlation

Scenario 6	**Incident Correlation Potentially Identifies Rapist**
Capability	Incident Correlation; Notification; Collaboration
Data	Incident Reports
Crime	Serial Rape
Functional Areas	Operational; Tactical
Scenario	Within a two week period, a rapist attacks two women in Pensacola, Florida. During the investigation, detectives discover that both cases have similar characteristics. Both victims were women in their 50s, living alone in ground floor apartments in adult-only complexes. In both attacks, the perpetrator broke into the victims' apartments through a window shortly before dawn on a Sunday and took the victims' drivers licenses when he left. One week later, police in Mobile, Alabama submit an incident report with similar characteristics, resulting in an N-DEx alert to the Pensacola Police Department. In this case, a witness saw a man in his 60s looking through a window of the victim's apartment the night before. The Pensacola investigator calls the Mobile PD to let them know of the similarity in cases, leading her to conclude that a serial rapist is involved. Using N-DEx, the Pensacola investigator sends out a bulletin to all police agencies in the Florida Panhandle and Southern Alabama about the related cases and authorities increase patrol vigilance during early morning hours. Among the cities that received the bulletin was Fort Walton Beach, Florida, about 40 miles east of Pensacola. The next Saturday morning, patrol officers in Fort Walton Beach observe a male in his 60s looking into the window of an apartment building. Officers apprehend the man who has glass cutters in his pocket and the driver's licenses of his past victims in his vehicle. Police in Fort Walton Beach submit his fingerprints to IAFIS and discover he is wanted for multiple rapes in other jurisdictions. During questioning, the man confesses to all three crimes.
Outcome	Using N-DEx's Incident /Case Correlation capabilities, police discover a pattern of linked crimes and predict an area where a rapist might strike next. Police apprehend a suspect, collect critical evidence and obtain a confession.

N-DEx Process that Allows Outcome



Incident Correlation/ Subscription Request
Characterization/ Comparison Against New Records
Characteristics Correlation Made/ Requester Notified
Incident/Case Correlation
OR

Incident/Case Correlation

Record: Incident 12345

Find Similar: ☑

Subscribe: ☑

Next

Crime Characteristics

Offense: Forcible Rape

Suspect: Male

Victim:

Race: White Height: 0 to 64

Sex: Female Weight: 0 to 130

Age: 55 to 65 Hair: Blonde

Find Similar: ☑

Subscribe: ☑

Next

Incident 12345

Offense:
Rape

Victim:
Sex: Female
Race: White
Age: 57
Height: 5' 1"
Weight: 120

Similar Cases

98% Pensacola, FL, Forcible Rape, 12 Dec 2005

95% Pensacola, FL, Forcible Rape, 19 Dec 2005

95% Mobile, AL, Forcible Rape 24 Dec 2005

88% Fort Walton Beach, FL,

Subscription Notification

Similar Crime Characteristics to your Incident 12345

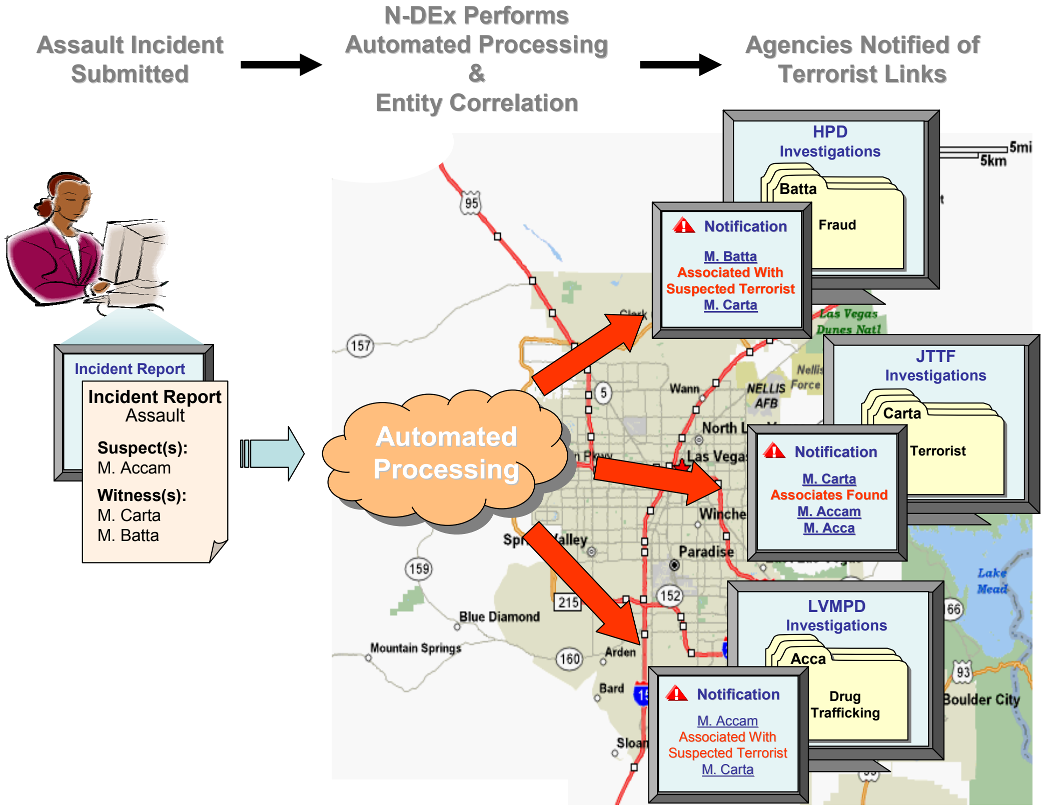
Mobile, AL, Forcible Rape, 19 Dec 2005

As depicted above, N-DEx's Subscription and Incident Correlation capabilities allowed the investigator to submit an incident to N-DEx and request notification any time police from other jurisdictions enter an incident with similar characteristics into N-DEx (agencies involved would be notified only if they configured their individual notifications accordingly). In this case, the similarities in the type of victim, location and time of day established a pattern. Because of this, police across the area increased vigilance and apprehended the suspect.

6.4 Automated Processing

Scenario 7	**Incident Report Links Drug Trafficker, Fraud Suspect and Suspected Terrorist**
Capability	Automated Processing; Entity Correlation; Notification; Collaboration
Data	Incident Reports; Case Reports
Crime	Providing material support or resources to designated foreign terrorist organizations
Functional Areas	Operational
Scenario	Mohammed Acca is a businessperson in Las Vegas, Nevada. He is known in the city for taking out large newspaper ads, soliciting funds to support peace in Lebanon. His T-shirt and souvenir shop produces $3 million a year in gross receipts. The Las Vegas Metropolitan Police Department believes Acca may be trafficking in illegal drugs, and has an open investigation. Mohammed Batta owns and operates an artifact and collectible store. In Boulder City, Nevada, the Boulder City Police Department has an investigation open on Batta, resulting from complaints about the authenticity of his merchandise. The JTTF at the FBI's Las Vegas office has long suspected that Mohammed Carta is a supporter of Hezbollah (a listed terrorist organization) and regularly sends the organization large sums of money. The JTTF does not know how Carta, a jewelry clerk, obtains these funds. When officers from the Henderson Police Department (HPD) respond to a disturbance call at a wedding, they find a man so badly beaten that he has to be airlifted to a hospital. A witness, who identifies himself as Mohammed Accam, has blood on his clothing. Mohammed Batta and Mohammed Carta also are present and interviewed as witnesses. They claimed to be brothers-in-law. The victim subsequently refuses to cooperate and all of the guests, including Accam, Batta and Carta, deny witnessing the beating. As a result, the investigation is stymied, but the incident report is submitted to N-DEx.
Outcome	When the incident from the disturbance call is entered into N-DEx by HPD, N-DEx makes the association between the three men and the three separate investigations and notifies each agency. Thus, N-DEx makes the connection between the terrorist suspect Carta, the artifact seller Batta, and the local suspected drug trafficker Acca.

N-DEx Process that Allows Outcome

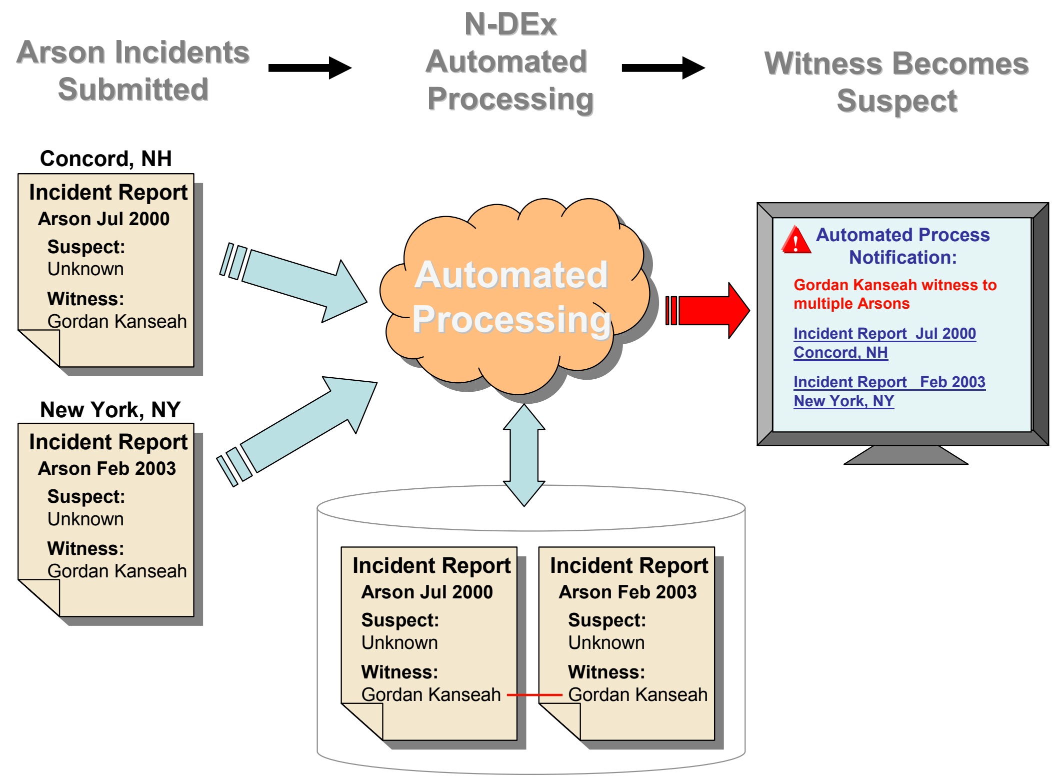


As depicted, the N-DEx Entity Correlation service correlates the seemingly unrelated activities and notifies the JTTF and investigators on all the cases of the link (agencies involved would be notified only if they configured their individual notifications accordingly). N-DEx Automated Processing identifies associations any time a new record is entered into N-DEx which correlates to another record or case. In this case, N-DEx automated processing is configured by all users so that any time information on a suspected terrorist is entered into N-DEx, including relationships to suspected terrorists, that the providers of the records be notified.

36

Scenario 8	**Automated Processing (Arson Witness)**
Capability	Automated Processing; Notification
Data	Incident Reports
Crime	Arson
Functional Areas	Tactical; Operational
Scenario	Fire investigators in Concord, New Hampshire respond to an abandoned warehouse fire. The evidence points to arson. Investigators interview people watching the fire and include their names in the incident report submitted to N-DEx. One of the witnesses is Gordan Kanseah. The case goes unsolved. Approximately three years later, fire investigators in New York City, New York arrive at a warehouse fire in which a night watchman has died. Gordan Kanseah is among the witnesses. Kanseah's name is included in a New York incident report submitted to N-DEx. N-DEx notifies both New York and New Hampshire authorities that the same person was a witness to both crimes.
Outcome	N-DEx provides investigators in Concord, NH and New York, NY a notification that a witness has shown up in multiple arson investigations, leading to a cooperative investigation that leads to Kanseah's arrest.

N-DEx Process that Allows Outcome

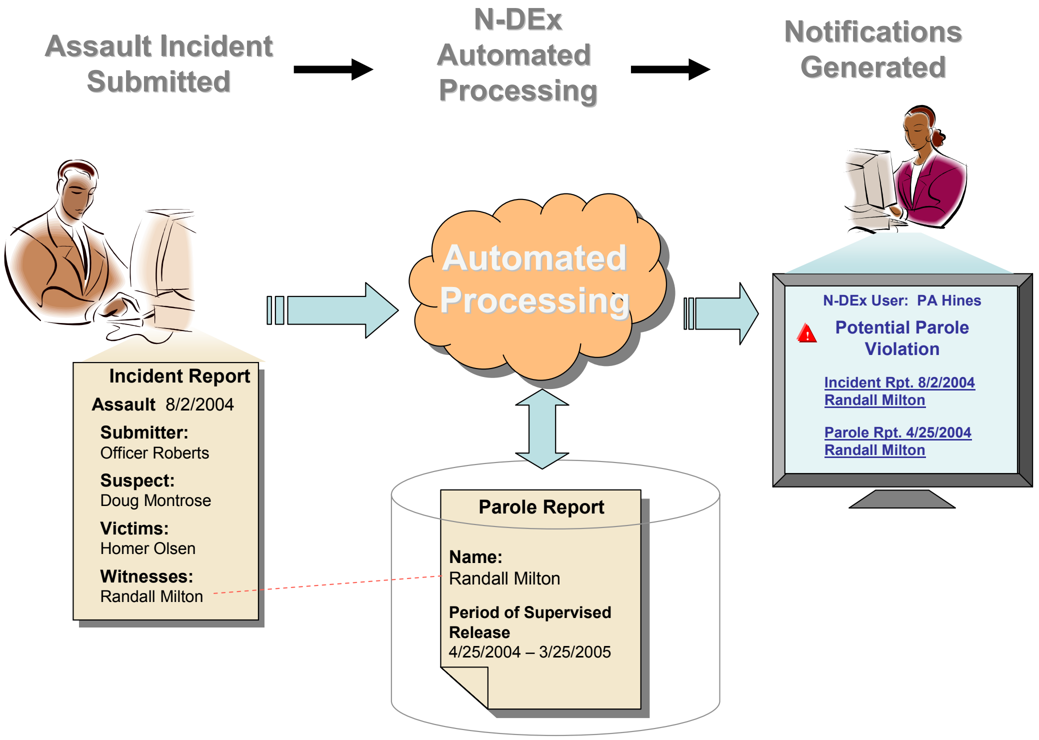


N-DEx's Automated Processing service discovers that a person is a witness in multiple arson investigations. N-DEx's automated processing services incorporate investigative best practices as an automated function so that all users can realize the benefit of these practices. In this case, N-DEx's automated function is programmed to look for a person that is found in multiple arson incidents as a suspect, witness or victim. Because of this automated process, both jurisdictions are then notified of the discovery (agencies involved would be notified only if they configured their individual notifications accordingly).

6

Scenario 9	Automated Processing (Parole Records)
Capability	Automated Processing
Data	Entity Correlation; Notification; Parole Records; Incident Report
Crime	Involuntary Manslaughter
Functional Areas	Tactical; Operational
Scenario	The Minnesota Department of Corrections releases Randall Milton from prison upon completion of his sentence for involuntary manslaughter resulting from a Driving while Intoxicated accident. Milton meets with his parole officer who enters a parole report into the RMS: the report is automatically submitted to N-DEx. The report includes information about Milton's address in Anoka, Minnesota, his place of employment, the requirement that he not use alcohol and not enter any liquor establishment. Previously, the parole officer had configured N-DEx to automatically notify him anytime one of his parolees' names appears in an incident. A month after Milton's release, an Eau Claire, Wisconsin police officer responds to a 911 call of a fight at an Eau Claire bar. Milton is among the witnesses interviewed. The police officer prepares an incident report about the incident, including participants in the fight and witnesses. N-DEx automatically notifies the parole officer that Milton was a witness to a barroom fight.
Outcome	After reviewing the incident report and speaking with the investigating police officer, the parole officer takes action to revoke Milton's parole.

N-DEx Process that Allows Outcome



Assault Incident Submitted → N-DEx Automated Processing → Notifications Generated

Incident Report

Assault 8/2/2004

Submitter:
Officer Roberts

Suspect:
Doug Montrose

Victims:
Homer Olsen

Witnesses:
Randall Milton

Automated Processing

Parole Report

Name:
Randall Milton

Period of Supervised Release
4/25/2004 – 3/25/2005

N-DEx User: PA Hines

Potential Parole Violation

Incident Rpt. 8/2/2004
Randall Milton

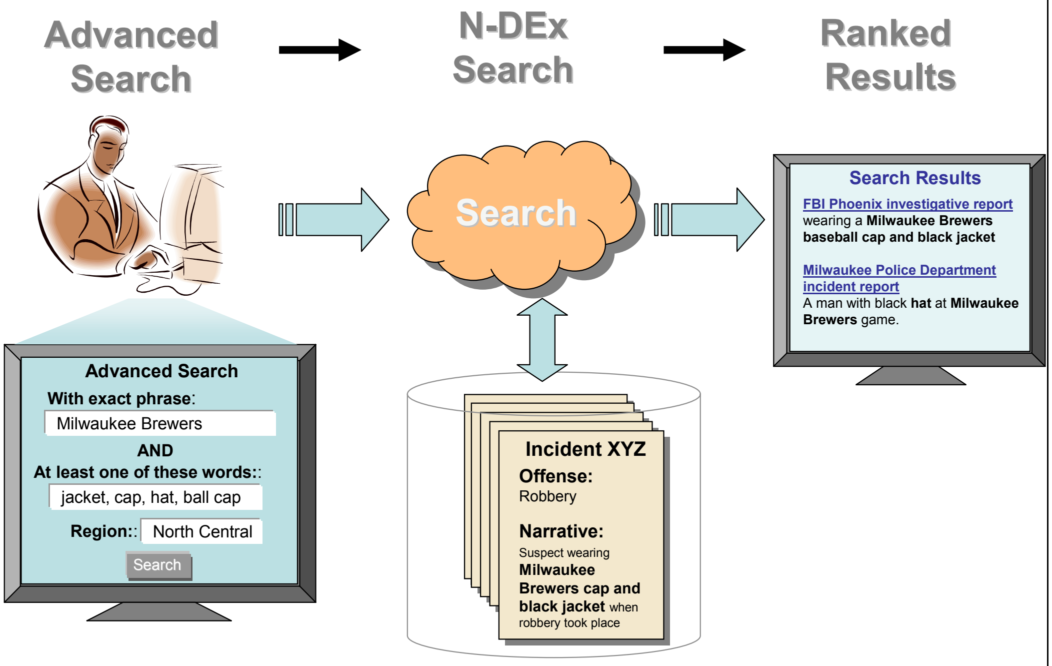
Parole Rpt. 4/25/2004
Randall Milton

As depicted, users can configure N-DEx to automatically notify them of events based on rule-based conditions. In this case, the user configured the system to identify any new records that involved a person on parole. This scenario is intended to show that the user can configure automated processes so that any time any person on parole is entered into N-DEx, that the user be notified. This is different from a subscription where the user subscribes to certain entities (in this case Randall Milton).

6.5 Search

Scenario 10	**Advanced Search – Narrative Search Brings Investigators Together**
Capability	Search (Advanced, Keyword/Phrase, Results Filtering); Entity Correlation
Data	Incident Report; Investigative Reports
Crime	Serial Armed Robbery
Functional Areas	Operational
Scenario	A Detroit Police Department detective is investigating a string of gas station robberies in which a male with a handgun threatens employees before fleeing with cash. The commonality to the robberies is that the man always wears a Milwaukee Brewers baseball cap and a black jacket. The detective searches N-DEx for the phrases " Milwaukee Brewers" and the words "jacket", "cap", "hat", or "ball cap." N-DEx returned too many results for effective analysis so the detective refined the search to specify a geographical area, Michigan and neighboring states. N-DEx locates a file about an FBI investigation in Chicago into a serial bank robber who wears a Milwaukee Brewers cap.
Outcome	N-DEx provides the Detroit detective with contact information for the FBI agent investigating the matter which potentially involves the same suspect.

N-DEx Process that Allows Outcome



Advanced Search → N-DEx Search → Ranked Results

Advanced Search

With exact phrase: Milwaukee Brewers

AND

At least one of these words:: jacket, cap, hat, ball cap

Region:: North Central

Incident XYZ

Offense: Robbery

Narrative: Suspect wearing **Milwaukee Brewers cap and black jacket** when robbery took place

Search Results

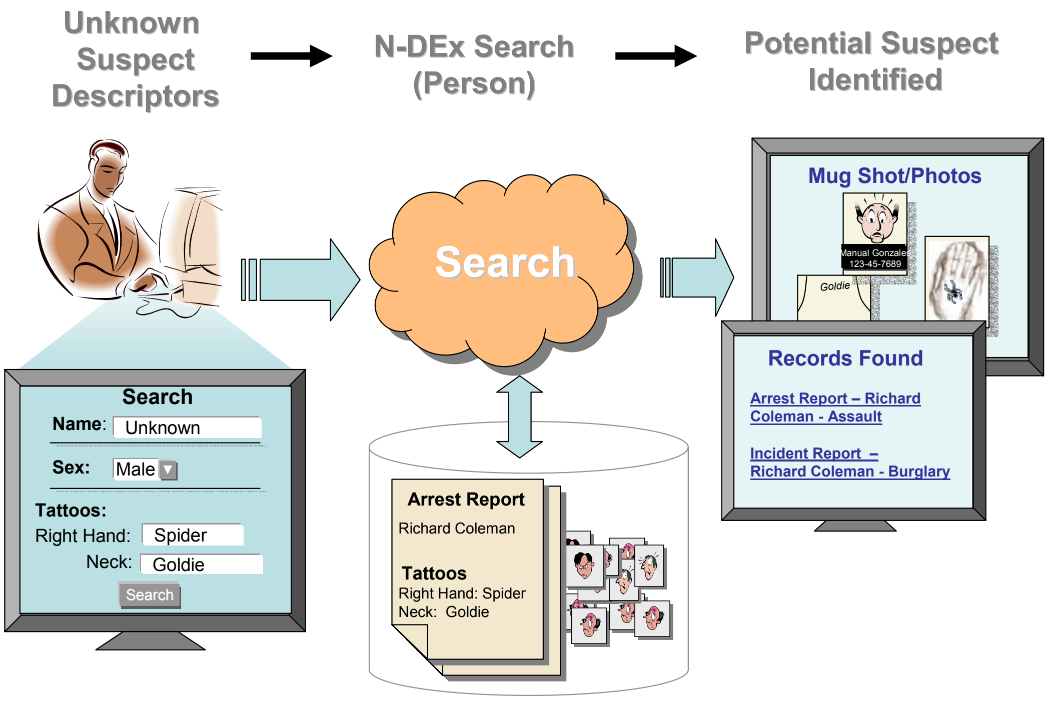
FBI Phoenix investigative report
wearing a **Milwaukee Brewers baseball cap and black jacket**

Milwaukee Police Department incident report
A man with black **hat** at **Milwaukee Brewers** game.

As depicted, N-DEx searches all records, including the available "narrative" information within incident records and produces a list of ranked results. This advanced search capability allows for filtering results and the production of a list of ranked results to the user. Since the words "Milwaukee Brewers" and "cap" and "jacket" are contained in the investigate report in close proximity, this record is ranked higher than other results.

Scenario 11	Search –Tattoo Identifies Home Invasion Suspect
Capability	Search; Visualization (mug shots, tattoo photos)
Data	Arrest/Booking Report; Criminal History; Incident Report
Crime	Home Invasion
Functional Areas	Operational
Scenario	Patrol officers in Los Angeles stop a vehicle for a traffic violation, discover it is a stolen vehicle and arrest the driver, Richard Coleman. During booking, police photograph Coleman's face and tattoos on his hand and neck. They enter a description and photographs of the tattoos into the booking record. Three weeks later, investigators in Denver are working a home invasion case where a male in a ski mask broke into the home of an elderly couple and beat and robbed them. Although they never saw his face, the victims told police the perpetrator had a spider tattoo on his right hand and the name "Goldie" tattooed across the back of his neck. Denver investigators perform an N-DEx search, using the only information they have – the sex of the perpetrator as well as the locations and descriptions of the tattoos.
Outcome	N-DEx locates a tattoo match in the Los Angeles booking report and returns information on the criminal history of Coleman, including descriptions, locations, and photographs of his tattoos and his mug shot. As a result, Denver investigators identify the perpetrator of a serious violent crime.

N-DEx Process that Allows Outcome



Unknown Suspect Descriptors → N-DEx Search (Person) → Potential Suspect Identified

Search

Name: Unknown

Sex: Male

Tattoos:

Right Hand: Spider

Neck: Goldie

Search

Search

Arrest Report

Richard Coleman

Tattoos

Right Hand: Spider

Neck: Goldie

Mug Shot/Photos

Manual Gonzales

123-45-7689

Goldie

Records Found

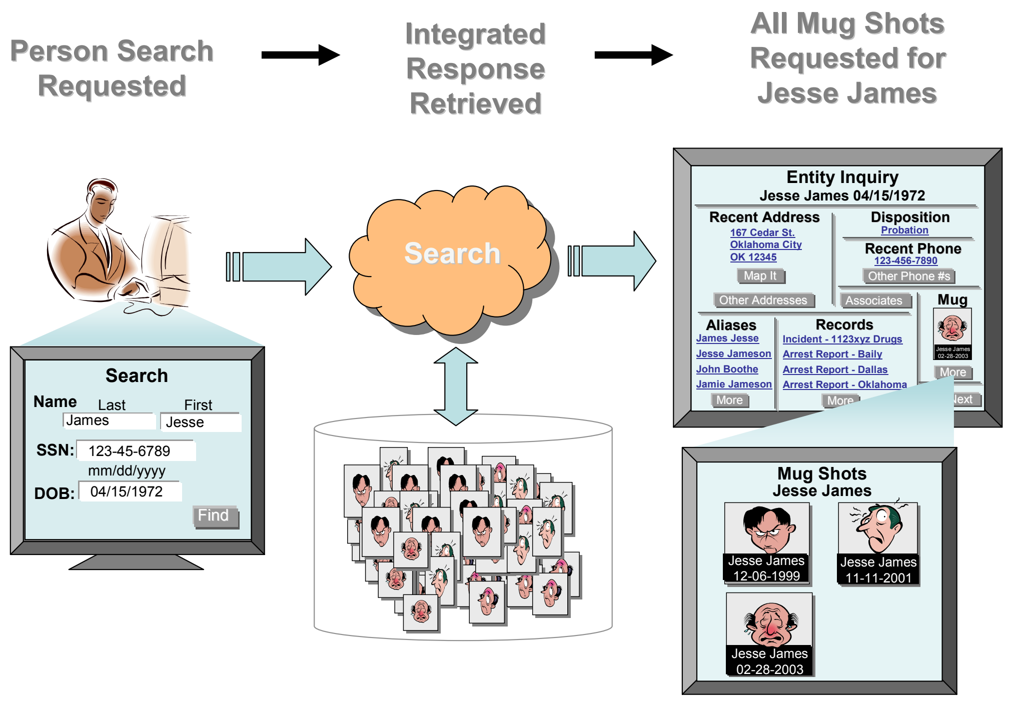
Arrest Report – Richard Coleman - Assault

Incident Report – Richard Coleman - Burglary

As depicted, the N-DEx Search capability enables investigators in one jurisdiction to find information that identifies a suspect arrested on an unrelated charge in another distant jurisdiction.

Scenario 12	**Search (Integrated Results/Mug Shot Retrieval**
Capability	Search, (Entity Inquiry - Person)
Data	Arrest/Booking Reports; Incident Reports; Criminal History Records
Crime	Drug Smuggling
Functional Areas	Operational
Scenario	The Drug Enforcement Administration (DEA) office in the U.S. Territory of Guam receives a tip that a narcotics trafficker named Jesse James is moving to Guam to set up a smuggling business. The tipster warns that James frequently changes his appearance.
Outcome	The DEA agent searches N-DEx for persons with the last name of James with drug investigations and discovers a person by the name of Jesse James has been arrested four times on drug charges in three different counties in Texas and one county in Oklahoma. The agent searches James' name and N-DEx displays integrated results, which includes a summary of all information concerning James including mug shot photographs that show how James changes his appearance over time. N-DEx displays arrest photographs of James from Matagorda County in 1999, Bailey County in 2001, and Dallas County in 2003, but Oklahoma County did not enter their mug shot of James into N-DEx. Access to these photos and other information (e.g., aliases) about James increases the probability that James will be recognized during a sting operation.

N-DEx Process that Allows Outcome



Person Search Requested → Integrated Response Retrieved → All Mug Shots Requested for Jesse James

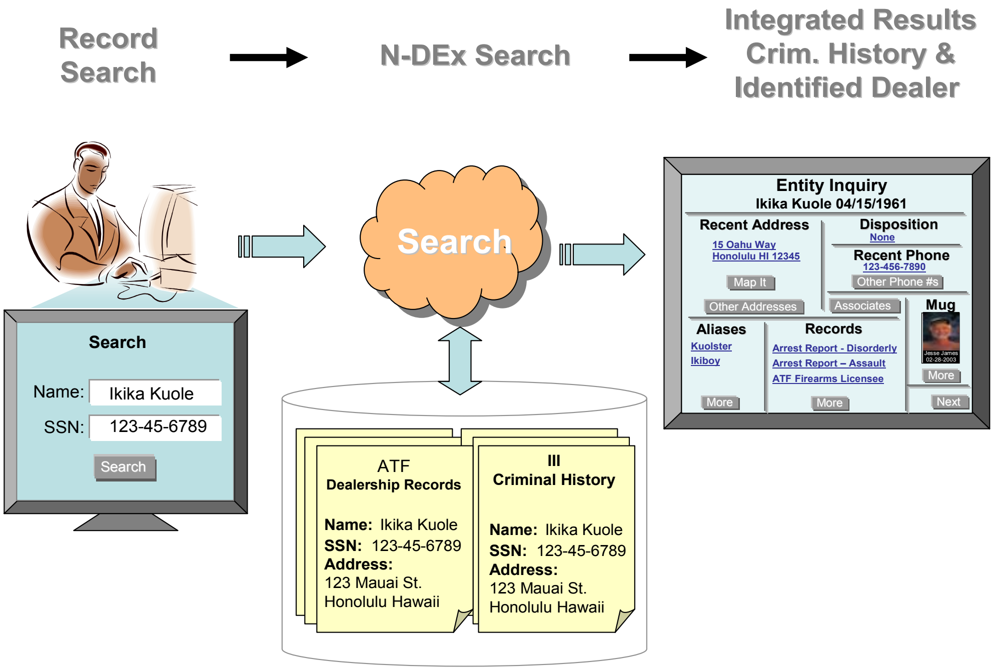
Search
Name Last: James First: Jesse
SSN: 123-45-6789
DOB (mm/dd/yyyy): 04/15/1972

Entity Inquiry
Jesse James 04/15/1972
Recent Address: 167 Cedar St. Oklahoma City OK 12345
Disposition: Probation
Recent Phone: 123-456-7890
Aliases: James Jesse, Jesse Jameson, John Boothe, Jamie Jameson
Records: Incident - 1123xyz Drugs, Arrest Report - Baily, Arrest Report - Dallas, Arrest Report - Oklahoma
Mug: Jesse James 02-28-2003

Mug Shots
Jesse James
Jesse James 12-06-1999
Jesse James 11-11-2001
Jesse James 02-28-2003

As depicted, N-DEx provides a summary of information on Jesse James from all the records available to N-DEx. (The integrated response can come from the information input into N-DEx as well as leveraging information available within systems such as NCIC, IAFIS, III, et.al.). The agent is able to select and view all mug shots from all records associated with Jesse James and hyperlinks to other records and files. For example, when the agent clicks on an alias, the record where that alias resides is retrieved.

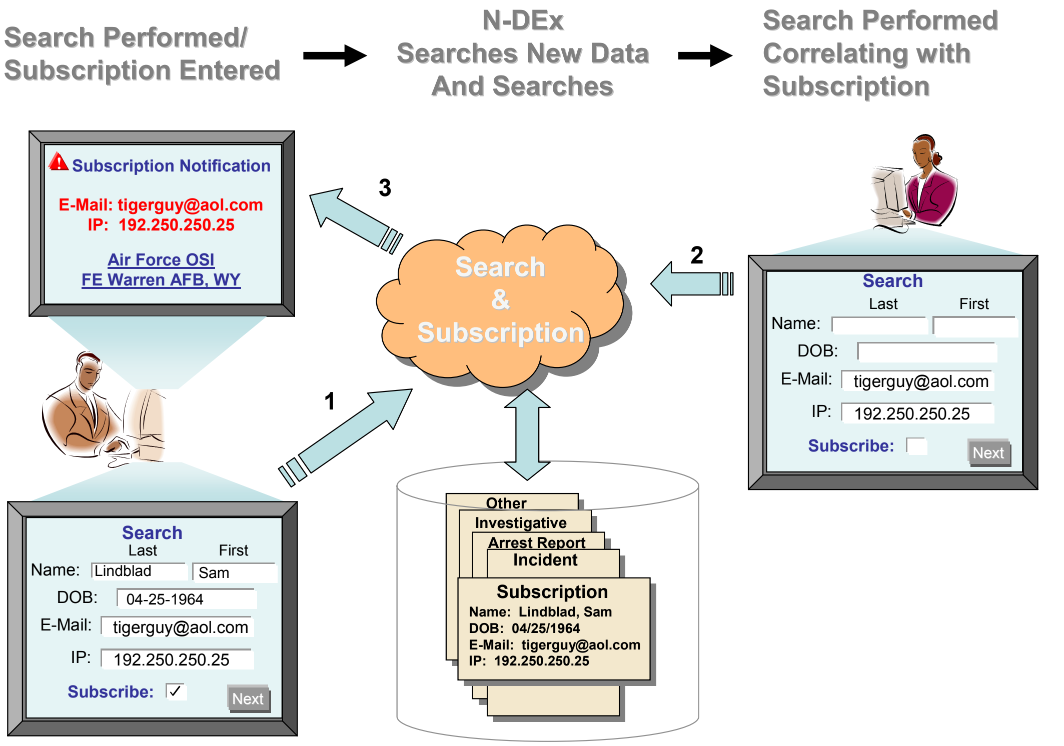
11

Scenario 13	**Search (Weapons Ownership)**
Capability	Search (Person)
Data	Federal Firearms Licensee (Firearms Dealer) Records; Criminal History
Crime	Check Fraud
Functional Areas	Tactical
Scenario	A White Collar Crime task force in Hawaii is making final preparations to serve an arrest warrant on Ikika Kuole for check fraud, which includes an N-DEx search. The search reveals that Kuole has a criminal history of misdemeanors for disorderly conduct and simple assault. N-DEx also reveals that Kuole has a federal firearms license.
Outcome	Because of Kuole's history of violence and firearms license, the task force elects to delay the scheduled arrest in order to change their plan.
N-DEx Process that Allows Outcome	 Record Search N-DEx Search Integrated Results Crim. History & Identified Dealer Search Search Map It Other Addresses Other Phone #s Associates More More More Next Search Name: Ikika Kuole SSN: 123-45-6789 ATF Dealership Records **Name:** Ikika Kuole **SSN:** 123-45-6789 **Address:** 123 Mauai St. Honolulu Hawaii III Criminal History **Name:** Ikika Kuole **SSN:** 123-45-6789 **Address:** 123 Mauai St. Honolulu Hawaii Entity Inquiry Ikika Kuole 04/15/1961 Recent Address: 15 Oahu Way Honolulu HI 12345 Disposition: None Recent Phone: 123-456-7890 Mug: Jesse James 02-28-2003 Aliases: Kuolster Ikiboy Records: Arrest Report - Disorderly Arrest Report – Assault ATF Firearms Licensee As depicted, N-DEx's Search capabilities reveal that a subject has a criminal record based on records in III and is a Federal Firearms Licensee based on Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) records. 28

6.6 Subscription

Scenario 14	Subscription– E-Mail and Internet Protocol (IP) Furthers Child Molestation Case
Capability	Subscription (Using E-Mail and Internet Protocol Addresses); Search
Data	User Queries of N-DEx
Crime	Sex Offender; Child Molestation
Functional Areas	Tactical; Operational (Investigations and Sting Operation)
Scenario	A detective in Bangor, Maine assigned to monitor a registered sex offender believes the man, Sam Lindblad, has been attempting to molest children again. The detective's suspicion was aroused after the manager of the apartment complex where Lindblad resides found an advertisement posted by Lindblad in the complex laundry room, offering to tutor children after school. When the detective went to Lindblad's apartment to question him, he noticed crayon drawings by children on the refrigerator and observed Lindblad cutting pictures of young boys out of catalogues. As no laws had been broken, the detective had to leave Lindblad's apartment. He returned to his office and searched for Lindblad's name in N-DEx using his identifiers to obtain information about Lindblad and to learn whether any other LEA had conducted an investigation on him. He also enters a subscription to be alerted of future activity on Lindblad. The detective included Lindblad's e-mail address of "tigerguy@aol.com" and Internet Protocol (IP) address in the subscription request. Six months later, N-DEx notified the detective when Lindblad's IP address had been queried on the system. A special agent with the Air Force Office of Special Investigations (AFOSI) at F.E. Warren Air Force Base in Wyoming, responded to a complaint by a service member that her 10-year-old son was being approached online by someone using the screen name "lionguy@aol.com" who she thought might be an adult. The text of the message, while stopping short of asking the child to meet the man for sex, was suggestive. The AFOSI agent did not believe he had enough evidence to seek a subpoena for the Internet Provider to obtain the true identity of the screen name so he entered the IP address into N-DEx as a search. N-DEx recognized the IP address from the Bangor subscription and notified both parties.
Outcome	Once notified of the investigation in Wyoming, the detective in Maine conducted an investigation to verify the IP address for Lindblad in Maine was the same one used in Wyoming. Based on a positive return, investigators' designed a sting operation that resulted in Lindblad's arrest.

N-DEx Process that Allows Outcome



Search Performed/ Subscription Entered → N-DEx Searches New Data And Searches → Search Performed Correlating with Subscription

1

Search

	Last	First
Name:	Lindblad	Sam
DOB:	04-25-1964	
E-Mail:	tigerguy@aol.com	
IP:	192.250.250.25	

Subscribe: ☑ Next

Search & Subscription

Other

Investigative

Arrest Report

Incident

Subscription

Name: Lindblad, Sam

DOB: 04/25/1964

E-Mail: tigerguy@aol.com

IP: 192.250.250.25

2

Search

	Last	First
Name:		
DOB:		
E-Mail:	tigerguy@aol.com	
IP:	192.250.250.25	

Subscribe: □ Next

3

Subscription Notification

E-Mail: tigerguy@aol.com

IP: 192.250.250.25

Air Force OSI

FE Warren AFB, WY

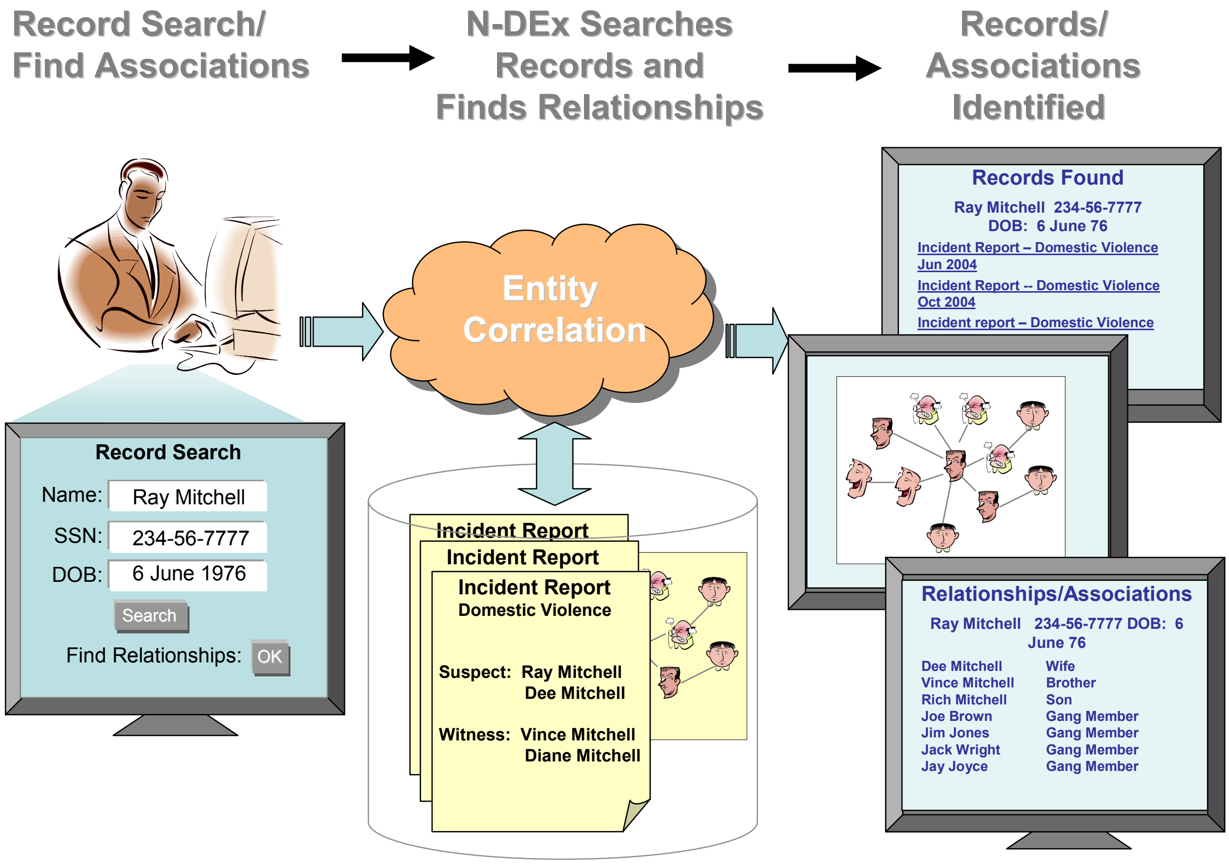
As depicted, the N-DEx Search capability allows investigators to search identifying information and descriptors about an entity and register a subscription for any records. If any N-DEx user searches for the same, or a similar entity, N-DEx notifies the user who set the subscription. In this case, the detective in Bangor was notified that another detective in Wyoming was performing a search of the IP address of the suspect.

34

6.7 Visualization

Scenario 15	Record Search & Relationships
Capability	Entity Correlation; Search (Person); Visualization
Data	Arrest/Booking; Incident Report
Crime	Murder
Functional Areas	Tactical; Operational
Scenario	Houston, Texas patrol officers arrest a man, who identifies himself as Ray Mitchell, on a charge of murder for killing another man in a bar fight. Mitchell provides arresting officers with a date of birth of June 6, 1976, an SSAN of 234-56-7777 and an address of 7 Elm Street, Dallas, Texas. During the booking process, arresting officer runs an NCIC and III check on the name Ray Mitchell and finds that Mitchell has an extensive criminal history. NCIC shows that there are fingerprints on file, but the man does not have any active arrest warrants. Mitchell is booked and fingerprinted and detectives submit his prints electronically to IAFIS. IAFIS responds that there are no fingerprint records on file for the person who is identifying himself as Mitchell. Detectives search N-DEx based on the data they have in an attempt to learn the true identity of the man. They display a visualization of Mitchell's past known relationships, and discover that on three occasions, officers from the Dallas PD have responded to the Elm Street address in Dallas on domestic disturbance calls. In two of those instances, police arrested Mitchell's stepfather for assaulting his wife. Responding officers included witness statements from family members in their arrest reports. One of the witnesses was Vincent Mitchell, Ray Mitchell's brother. Detectives obtain a drivers license photograph of Vincent, using standard police procedures separate from any N-DEx processes. The photograph reveals the person in custody in Houston was actually Vincent Mitchell; not his brother, Ray Mitchell.
Outcome	N-DEx helps police discover the true identity of a man charged with murder as the result of information provided to N-DEx from another jurisdiction.

N-DEx Process that Allows Outcome



Record Search/ Find Associations → N-DEx Searches Records and Finds Relationships → Records/ Associations Identified

Record Search

Name: Ray Mitchell

SSN: 234-56-7777

DOB: 6 June 1976

Search

Find Relationships: OK

Incident Report

Incident Report

Incident Report
Domestic Violence

Suspect: Ray Mitchell
Dee Mitchell

Witness: Vince Mitchell
Diane Mitchell

Records Found

Ray Mitchell 234-56-7777
DOB: 6 June 76

Incident Report – Domestic Violence
Jun 2004

Incident Report -- Domestic Violence
Oct 2004

Incident report – Domestic Violence

Relationships/Associations

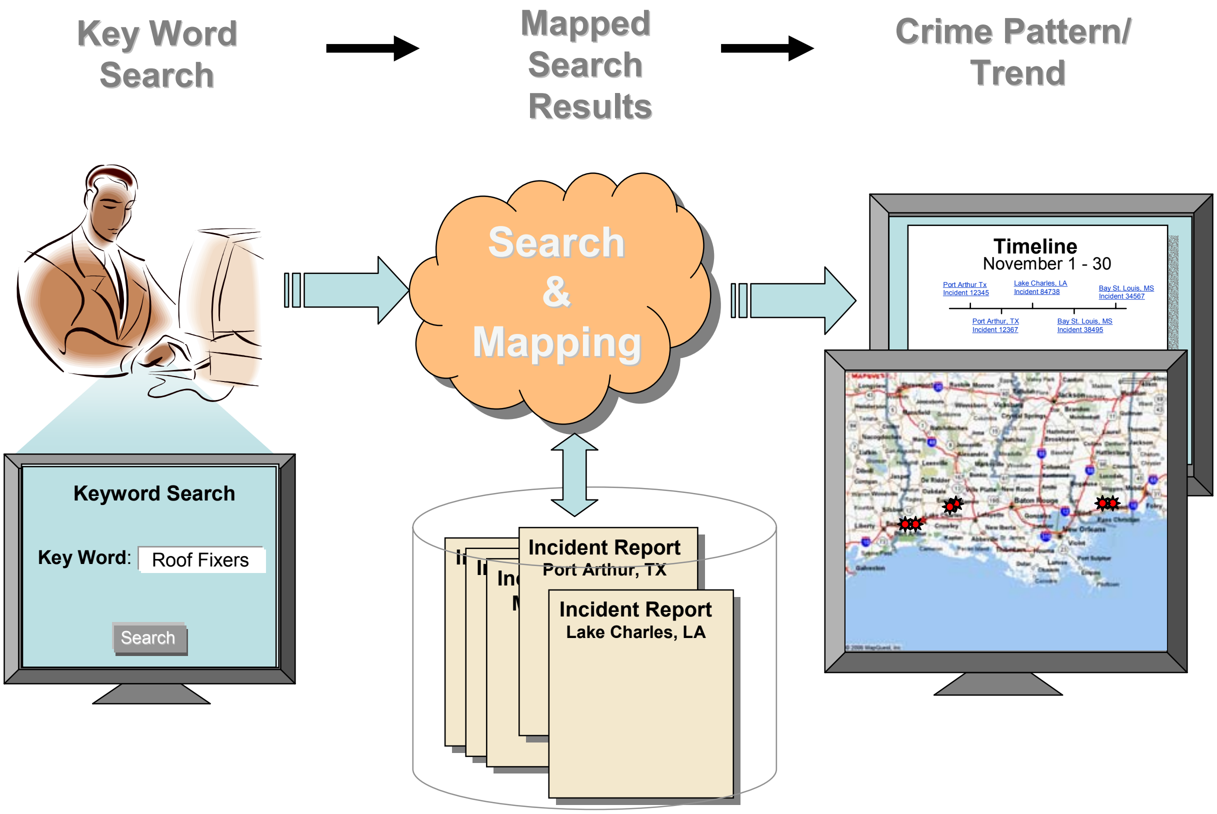
Ray Mitchell 234-56-7777 DOB: 6 June 76

Dee Mitchell	Wife
Vince Mitchell	Brother
Rich Mitchell	Son
Joe Brown	Gang Member
Jim Jones	Gang Member
Jack Wright	Gang Member
Jay Joyce	Gang Member

As depicted, N-DEx provides the capability to search for records based on personal identifiers and determine associations and relationships between people contained in multiple incident reports. (The integrated response can come from the information input into N-DEx as well as leveraging information available within systems such as NCIC, IAFIS, III, et.al.). Cross jurisdictional searching of records assists in resolving that the person in custody is Vincent Mitchell and that Ray Mitchell and Vincent Mitchell are two different people.

Scenario 16	**Key Word Search and Results Mapping Stops Hurricane Fraud**
Capability	Visualization (Geographic Mapping, Timelines); Search (Keyword); Collaboration; Entity Correlation (Vehicle to Location)
Data	Incident Reports
Crime	Fraud
Functional Areas	Operational; Tactical
Scenario	The Gulfport, Mississippi Police Department receives five complaints in a single day from citizens who paid a contractor in advance to repair hurricane roof damage, but he never came back to do the work. The callers all said that a white male solicited them at their door. He said he could fix their roof that afternoon, but needed $200 in advance to purchase supplies. The man said he would leave his toolbox containing expensive tools as collateral. But the man never returns and the victims find the toolbox empty. None of the callers know the man's name, but one recalls seeing a magnetic sign on the door of the truck which read "Roof Fixers." The detective searches N-DEx for "Roof Fixers." N-DEx returns previously reported similar incidents from Port Arthur, Texas, Lake Charles, Louisiana and Bay St. Louis, Mississippi which contained the phrase "Roof Fixers." The detective then used N-DEx to display the incident locations on a map along with date/time of the incidents. From the displayed map, the detective discovers that the similar complaints all occurred within days of each other along the Interstate 10 corridor that sustained damage from Hurricane Katrina. From the map, Gulfport police project that Biloxi, Mississippi could be the next target of the fraud perpetrator. Gulfport police telephone Biloxi police, advise them of the trend, and issue an Nlets bulletin and an N-DEx notification message. Contained in the Nlets and N-DEx bulletins/alerts is a notification that additional details relative to the investigation of the "Roof Fixers" scam are available and can be viewed in N-DEx using collaboration tools.
Outcome	The Biloxi Police Department provides their street patrols with a description of the man and the vehicle. A day later, a patrol officer arrests the subject while he is attempting to negotiate a roof repair in a hurricane-damaged Biloxi neighborhood.

N-DEx Process that Allows Outcome



Key Word Search

Mapped Search Results

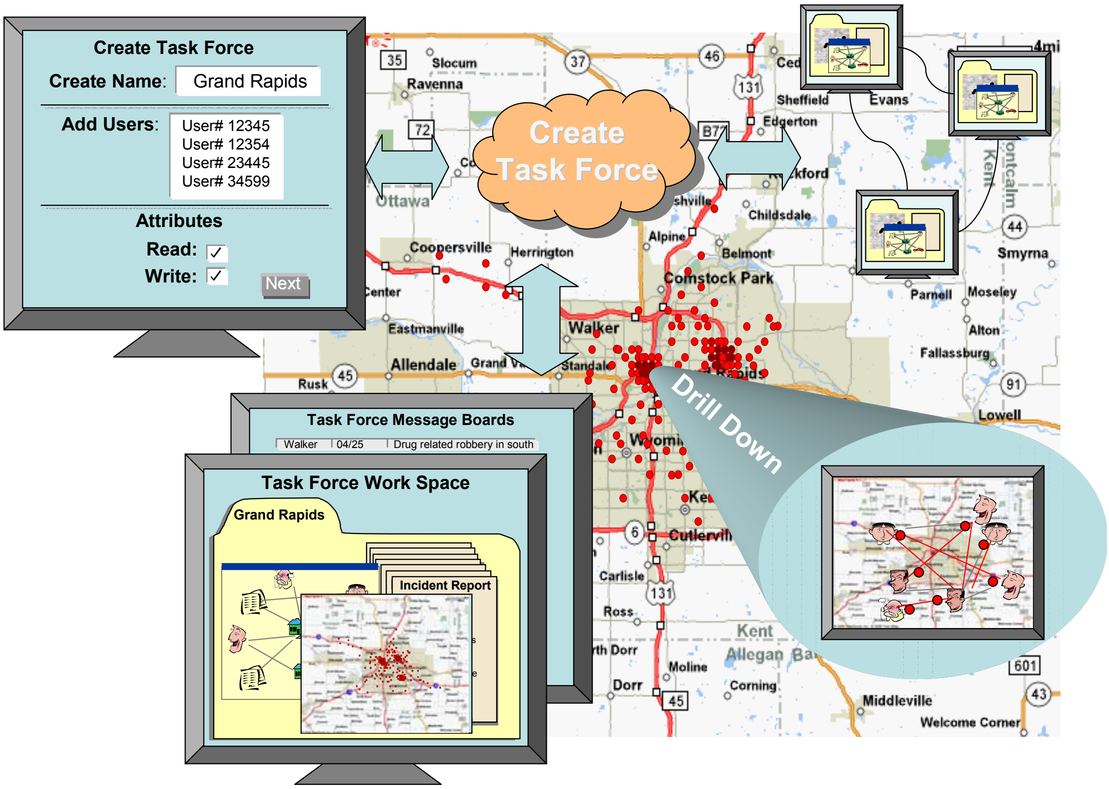
Crime Pattern/ Trend

As depicted, N-DEx's Search capabilities retrieve all records with incidents that include "Roof Fixers" and all incidents show similar complaints. N-DEx Visualization capabilities are used to display a trend for these crimes over time showing movement along I-10 towards Biloxi, Mississippi. The Collaboration capability allows N-DEx to store the compiled information/research in an agency case file which can be shared with interested investigative parties.

9

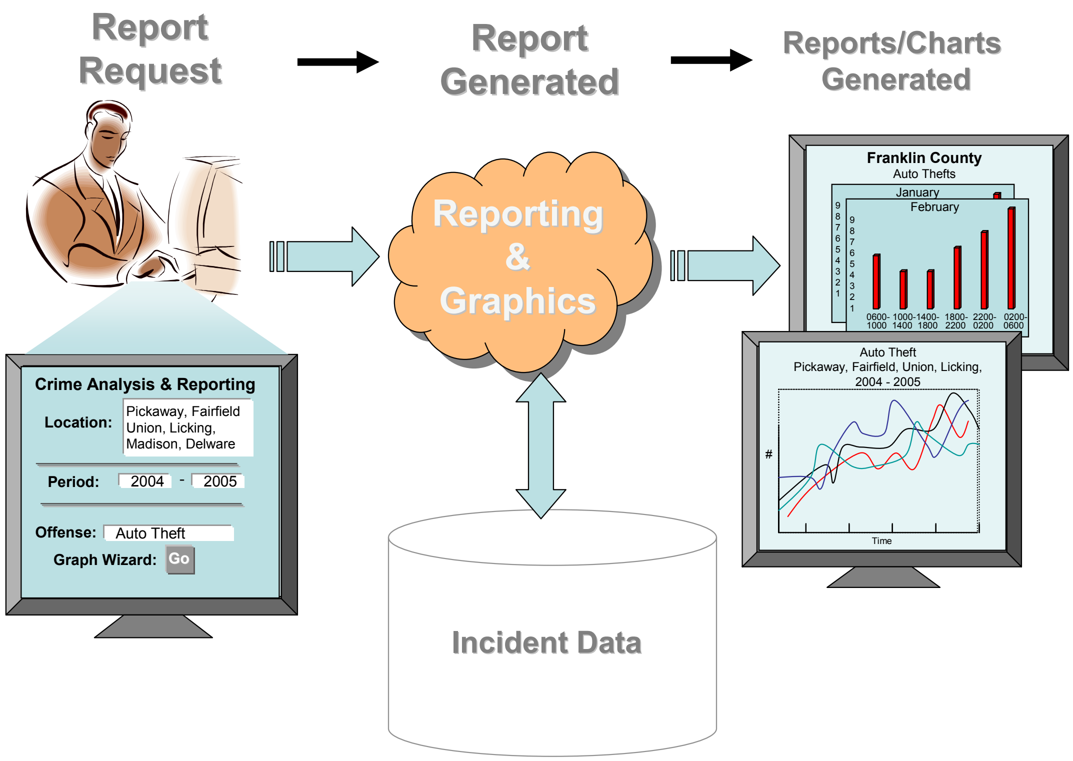
6.8 Analytical/Reporting and Collaboration

Scenario 17	**Analytical/Reporting ("Hot Spot"/"Drill Down")**
Capability	Analytics; Visualization; Incident Correlation; Collaboration
Data	Incident Reports; Field Reports; Case Investigations; Analytic Reports
Crime	Burglary; Robbery; Car Theft; Narcotics
Functional Areas	Strategic; Administrative; Operational
Scenario	Police are investigating a series of robberies and burglaries spanning three jurisdictions around Grand Rapids, Michigan. The investigation involves two detectives from the Kent County Sheriff's Department (KCSD) Criminal Investigation Bureau and several patrol deputies. Additionally, the Kentwood Police Department is investigating one case while the Criminal Unit of the Grand Rapids Police Department is investigating two others. Police have not identified the perpetrators and have little or no physical evidence. Based on incident and field reports on each crime report entered into N-DEx, KCSD investigators using both the analytics and incident correlation capabilities, discover that a pattern extends beyond their cases into the neighboring jurisdictions. Investigators from all three agencies agree to create a collaborative workspace within N-DEx, and begin to share reports and other related investigation information. The KCSD designates one investigator as the lead investigator with responsibility for gathering additional case information from the other jurisdictions and creating analytical reports for the multi-jurisdictional team. Using the N-DEx analysis and visualization capabilities, the lead investigator plots the location of the crimes, which N-DEx automatically correlates and then presents the results on a map that shows "hot spots" throughout the cities in question. These analytical results are presented to the remaining team members for further analysis. The team "drills down" on the "hot spots" to discover if there are other crime attributes or relationships between their cases and other criminal activities within the "hot spots." The team learns that thieves previously abandoned a stolen car used in the crimes near several of the robberies and burglaries. They determine that many of the stolen cars came from a neighborhood located in western Kent County, near the City of Kentwood. A closer examination, using N-DEx's visualization capability and analytical charting tools, reveals that many of these crimes also can be linked by the time of day and days of the month. The investigation team documents these findings and disseminates this information to the appropriate supervisors within each agency (and other neighboring law enforcement jurisdictions).

Outcome	The joint investigation facilitated by N-DEx's capabilities and services leads to a group of crack cocaine addicts working out of Kentwood, resulting in multiple arrests for robbery, burglary, drug possession and car theft in multiple locations along a path between Kentwood and downtown Grand Rapids, in Kent County, Michigan.
N-DEx Process that Allows Outcome	 Create Task Force Create Name: Grand Rapids Add Users: User# 12345 User# 12354 User# 23445 User# 34599 Attributes Read: ✓ Write: ✓ Next Task Force Message Boards Walker 04/25 Drug related robbery in south Task Force Work Space Grand Rapids Incident Report Create Task Force Drill Down Slocum Ravenna Ottawa Coopersville Herrington Eastmanville Allendale Grand Va Rusk Walker Standale Alpine Comstock Park Belmont Childsdale Edgerton Sheffield Evans Smyrna Parnell Moseley Alton Fallassburg Lowell Kent Allegan Carlisle Ross Moline Dorr Corning Middleville Welcome Corner 35 37 46 131 72 45 44 91 601 43 6 As depicted, N-DEx allows investigators to discover relationships between multi-jurisdictional crimes. The Collaboration capability allows multiple agencies to share information on matters of mutual interest to further empower N-DEx's Analytical and Visualization capabilities. Investigators are able to match additional cases and information in a joint effort, and then focus on crime relationships within regional "hot spots." The Incident Correlation service helps investigators in multiple jurisdictions bridge the connections between crimes, cases and activities within each of their agencies. 35

Scenario 18	**Crime Trend & Pattern Reporting / Presentation**
Capability	Analytical/Reporting; Visualization (Trend Graphs); Collaboration
Data	Incident Report
Crime	Auto Theft
Functional Areas	Operational; Tactical; Strategic; Administrative
Scenario	A Franklin County, Ohio Sheriffs Department crime analyst issues a report, showing a 66 percent spike in automobile thefts, resulting in a request for further analysis. One key question is whether the increase is isolated to Franklin County, or extends to surrounding counties. The analyst uses N-DEx to create a report of auto thefts from his county and the six surrounding counties of Pickaway, Fairfield, Union, Licking, Madison, and Delaware over the last 12 months. N-DEx produces a report that identifies the auto thefts in the area by number, day of the week, time of day and month, and visually displays the output graphically. The report indicates that Union and Fairfield counties have suffered a similar trending spike in auto thefts, but the other three counties have actually seen a decrease.
Outcome	The Franklin County Sheriff contacts his counterparts in the other counties, creates a joint task force and redeploys his resources to focus more on auto thefts. N-DEx is also used to create a collaboration zone to help the task force share information and manage the investigation.

N-DEx Process that Allows Outcome



Report Request → Report Generated → Reports/Charts Generated

Crime Analysis & Reporting

Location: Pickaway, Fairfield Union, Licking, Madison, Delware

Period: 2004 - 2005

Offense: Auto Theft

Graph Wizard: Go

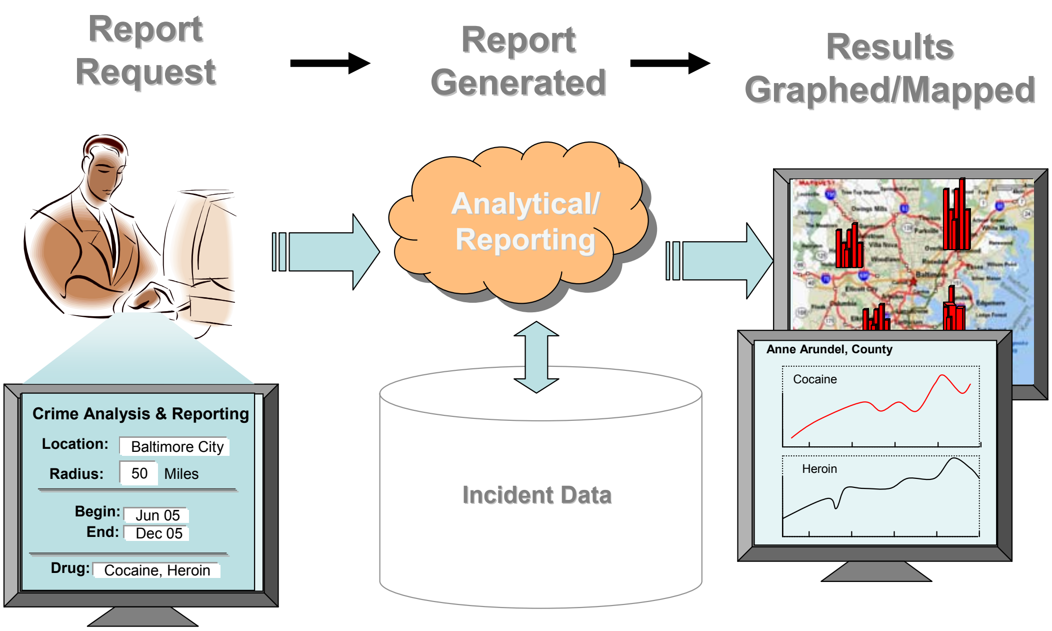
Reporting & Graphics

Incident Data

As depicted, N-DEx's Analytical/Reporting and Visualization capabilities aid crime analysts in presenting information to management to support strategic planning and investigation and patrol activities.

16

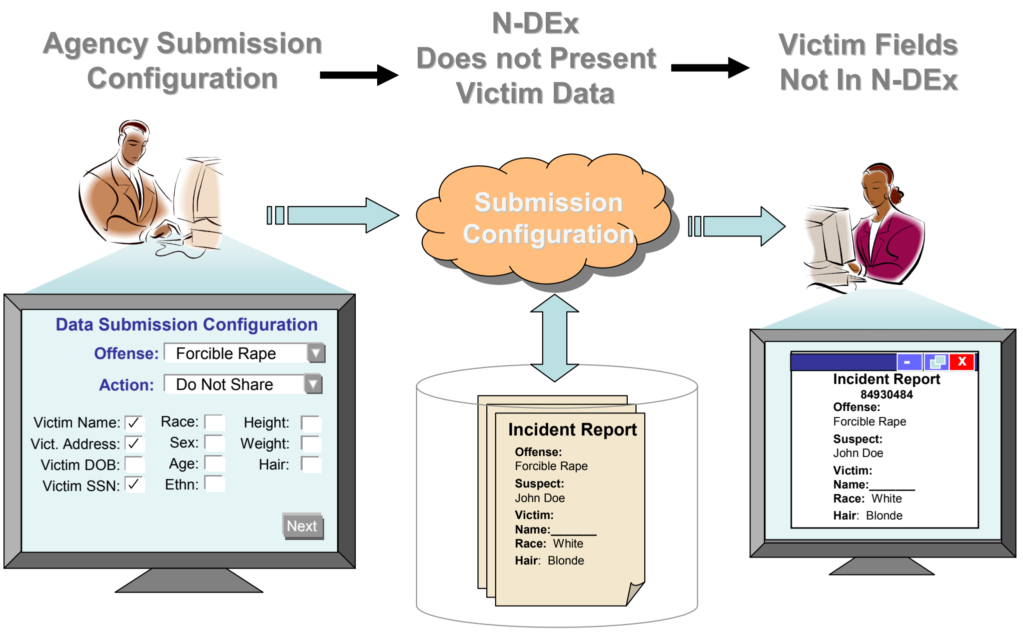
Scenario 19	Analytical/Reporting (Drug “Hot Spots”)
Capability	Analytical/Reporting; Visualization; Collaboration
Data	Incident Reports
Crime	Murder; Drug Trafficking; Robbery
Functional Areas	Strategic; Operational
Scenario	A Baltimore Police Department lieutenant oversees the Planning and Research Department which includes strategic planning. This strategic planning concerns crime trends, crime movement, crime mapping, and other related analytical tools, which are used by the Police Department to develop and set priorities, make resource allocation, and predict crime. Over the last year, the department has been targeting open air drug markets. Over this time, the lieutenant has noticed a significant increase in drug-related incidents and arrests for the first half of the year followed by a dramatic decrease in arrests over the last half of the year. Meanwhile, he has seen robberies and murders remain stable for the first half of the year and then begin to rise in the second half of the year. These trends are counter to Baltimore’s historical trends where robberies and murders tend to decrease with a crackdown on drug trafficking. The lieutenant uses N-DEx to map the occurrences of robberies and murders that occurred in the city over the last half of the year. He then uses N-DEx to map all Baltimore city addresses for people, vehicles, and other entities identified in drug related incidents occurring in adjacent jurisdictions over the last half of the year. The results show a pattern where the areas in the city with an increase in murders and robberies are consistent with the areas where addresses are identified from drug related incidents occurring in the adjacent jurisdictions. Based on this information, the lieutenant concludes that the city's crackdown on drug trafficking is leading users and dealers who resided in Baltimore to go to adjacent jurisdictions to buy and sell drugs. This increase in drug demand in adjacent jurisdictions is causing the price to increase. As a result, Baltimore city users’ drug cost increased. To pay for this increase, users are conducting more robberies to acquire the additional money needed to purchase drugs. Meanwhile, Baltimore city dealers are attempting to sell more of their drugs in adjacent jurisdictions where other drug dealers already operate resulting in more drug-related murders.

Outcome	The lieutenant prepares a strategic report on the trend information he has gathered from N-DEx. This results in the creation of a regional drug task force which uses N-DEx to collaborate confidentially on investigations.
N-DEx Process that Allows Outcome	 Report Request Report Generated Results Graphed/Mapped Analytical/ Reporting Incident Data Anne Arundel, County Cocaine Heroin Crime Analysis & Reporting Location: Baltimore City Radius: 50 Miles Begin: Jun 05 End: Dec 05 Drug: Cocaine, Heroin As depicted, N-DEx Visualization capabilities allow users to generate graphical representations of various views of incident data to support strategic crime analysis. 26

6.9 Authorization

Scenario 20	Authorization (Rape Victim Information)
Capability	Authorization (Privacy); Search (Records)
Data	Incident Report
Crime	Rape
Functional Areas	Operational
Scenario	An LEA wants to share incident data in N-DEx, but has a state law that prohibits unauthorized dissemination of victim information from records containing information of rape victims.
Outcome	N-DEx is configured at the appropriate agreed upon level (user, agency, state, national) so incident reports on rape cases precludes the sharing of data elements about the victim. When a user from another agency accesses the incident report, N-DEx excludes victim identifying information (e.g., name, address, SSAN), but is able to share information on other aspects of the entity.

N-DEx Process that Allows Outcome



Agency Submission Configuration → N-DEx Does not Present Victim Data → Victim Fields Not In N-DEx

Data Submission Configuration

Offense: Forcible Rape

Action: Do Not Share

Victim Name:	☑	Race:	□	Height:	□
Vict. Address:	☑	Sex:	□	Weight:	□
Victim DOB:	□	Age:	□	Hair:	□
Victim SSN:	☑	Ethn:	□		

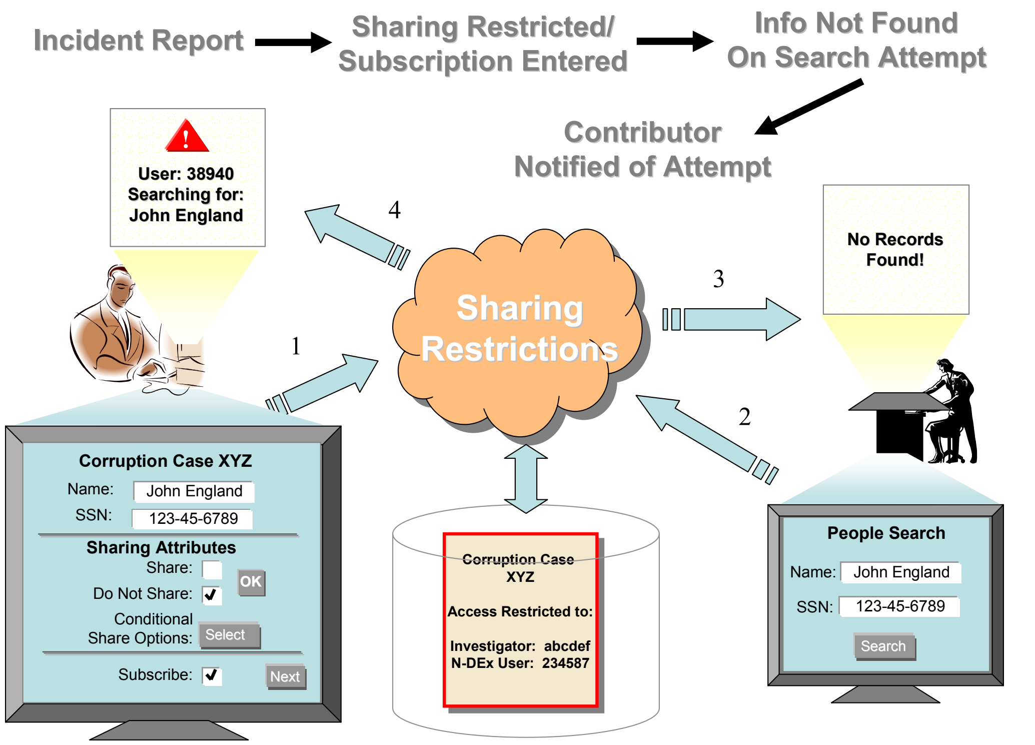
Incident Report
Offense:
Forcible Rape
Suspect:
John Doe
Victim:
Name:_______
Race: White
Hair: Blonde

Incident Report
84930484
Offense:
Forcible Rape
Suspect:
John Doe
Victim:
Name:_______
Race: White
Hair: Blonde

As depicted, the N-DEx system is configurable at the appropriate agreed upon level (user, agency, state, national) so that victim information in records with an offense code of forcible rape (for example) is recognized and excludes victim information from sharing. N-DEx will allow for the maximum flexibility in configuring the system to promote information sharing.

Scenario 21	**Protecting Information (Public Corruption)**
Capability	Authorization (Privacy); Search; Subscription
Data	Incident Reports
Crime	Public Corruption
Functional Areas	Operational
Scenario	While attending a social event, the Sheriff of Smith County, Idaho overhears a construction company owner, John England, boast to another guest that he paid a school superintendent $5,000 to obtain a contract to re-roof the county's high school. The sheriff calls the Idaho State Police to report the incident. The state police assign an investigation team to the case. When members of the team complete reports on the case, they submit them to N-DEx and limit the ability of N-DEx to share the reports by setting the appropriate record attributes, restricting access only to team members. A week later, England approaches a deputy with the Smith County Sheriff's Office and convinces the deputy to search the agency's records for his name or the superintendent's name. The deputy searches N-DEx for the contractor's name and the superintendent's name. The system returns no responses. However, the system notifies the Idaho State Police of the search.
Outcome	N-DEx allows data owners to restrict access to the data they submit to the system and notifies data owners when others try to access the restricted data. In this case, N-DEx allowed the state police to build a new case against the contractor and the deputy who helped him misuse the system.

N-DEx Process that Allows Outcome


Incident Report
Sharing Restricted/ Subscription Entered
Info Not Found On Search Attempt
Contributor Notified of Attempt
Sharing Restrictions
1
2
3
4

User: 38940
Searching for:
John England

No Records Found!

Corruption Case XYZ

Name: John England
SSN: 123-45-6789

Sharing Attributes

Share: □
Do Not Share: ☑
OK
Conditional Share Options: Select
Subscribe: ☑
Next

Corruption Case XYZ

Access Restricted to:

Investigator: abcdef
N-DEx User: 234587

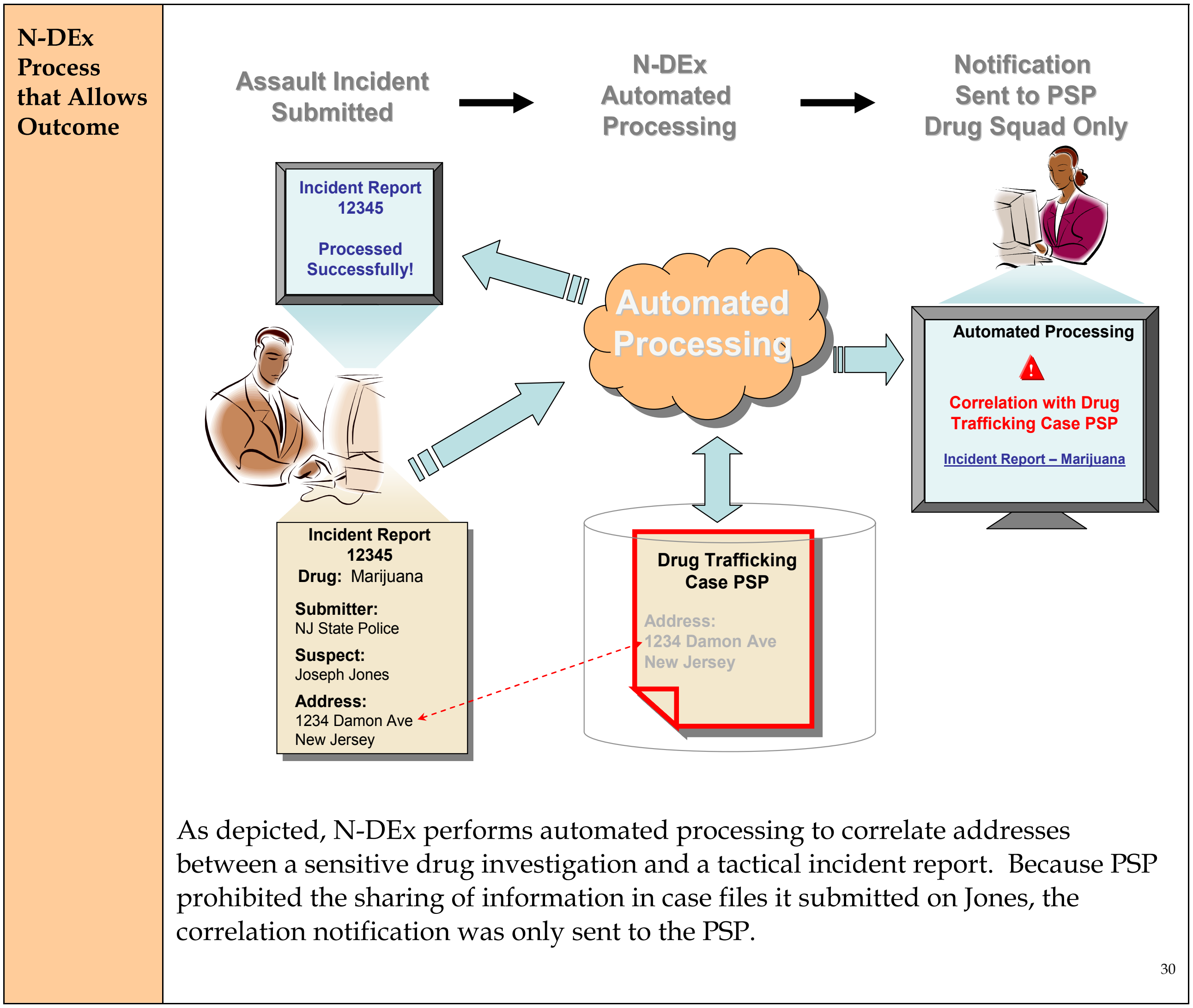
People Search

Name: John England
SSN: 123-45-6789
Search

As depicted, N-DEx restricts access to data when the contributor chooses to control access to the data. Additionally, the system alerts the contributor when others try to search and/or retrieve information about the restricted data.

13

Scenario 22	Authorization (Data Ownership Security)
Capability	Authorization; Automated Processing
Data	Incident Report; Case File
Crime	Drug Trafficking
Functional Areas	Tactical; Operational
Scenario	A New Jersey State Police (NJSP) officer stops Joseph Jones for speeding on the New Jersey Turnpike. After obtaining Jones' permission, the officer searches the vehicle and finds marijuana. He arrests Jones for the marijuana possession. The NJSP submits an incident report to N-DEx on the stop and arrest. N-DEx notifies the Pennsylvania State Police (PSP) that the home address provided by Jones correlates to an address in a case it is working, involving a high-level member of a drug trafficking organization.
Outcome	Because the PSP chose to control access to the drug trafficking case due to its sensitivity, N-DEx does not allow NJSP to see the correlation nor notify NJSP about the correlation, giving PSP the control to evaluate whether or not to contact the NJSP about Jones.



N-DEx Process that Allows Outcome

As depicted, N-DEx performs automated processing to correlate addresses between a sensitive drug investigation and a tactical incident report. Because PSP prohibited the sharing of information in case files it submitted on Jones, the correlation notification was only sent to the PSP.

30

7 System Overview

This section introduces the N-DEx system conceptually. It addresses data and functional integration, network connectivity and provides examples of options for agencies to integrate with N-DEx. *Figure 7-1* notionally depicts N-DEx data and functional integration. It serves for discussion purposes only and is not meant to indicate a particular design solution.

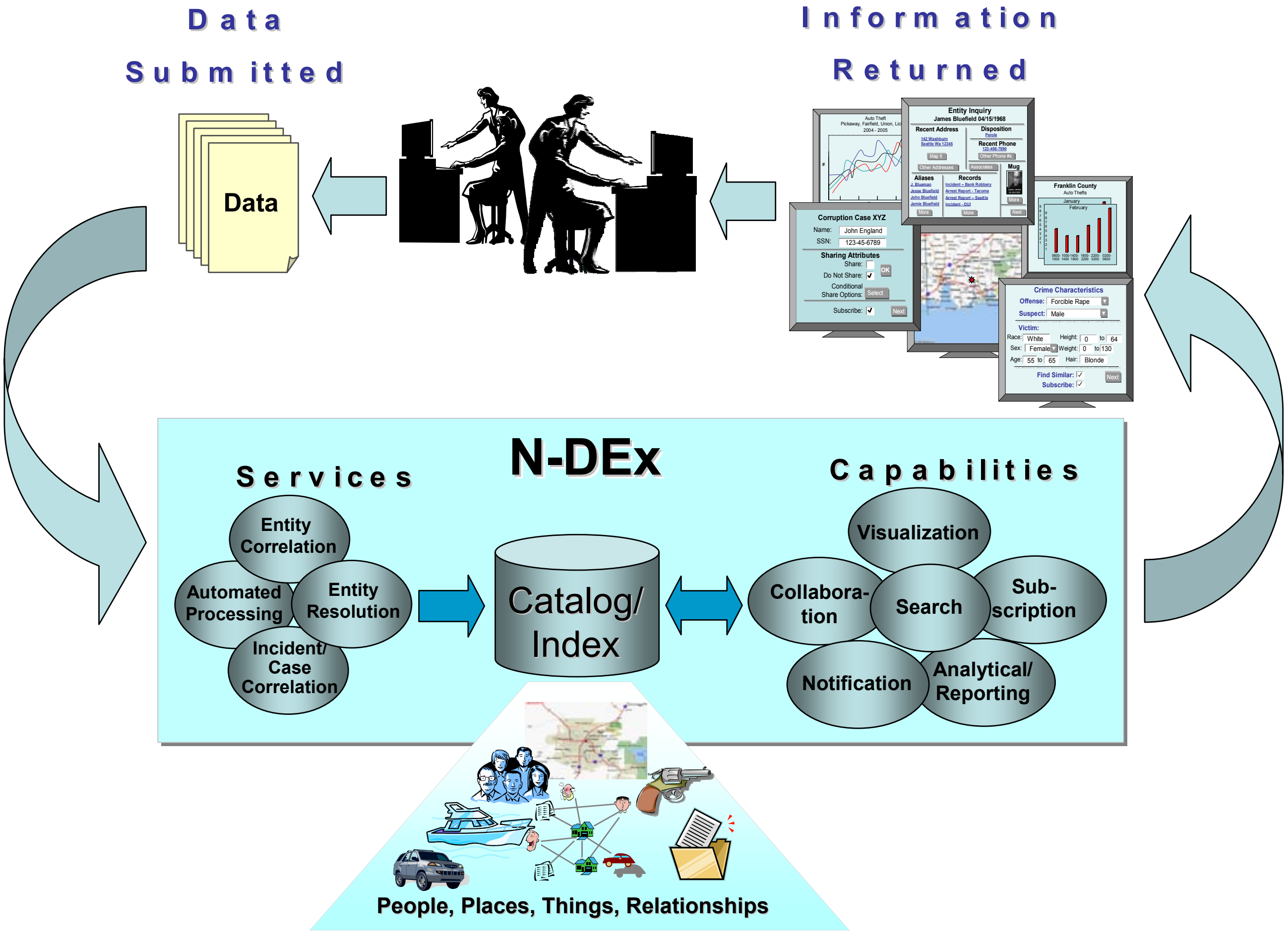


Figure 7-1. N-DEx Conceptual System

N-DEx is a national scale system for sharing diverse law enforcement information currently housed in various information systems in a number of formats across the country, while maintaining privacy and security. N-DEx will act upon this data to gather information, discover relationships among the information and provide useful knowledge to N-DEx users throughout the Nation as illustrated above.

All information shared through N-DEx originates from data supplied by data sources from numerous local, state, tribal and federal systems to include, but not be limited to: incident reports, arrest reports, case files, booking reports, incarceration records and criminal histories.

These records contain information about entities (e.g., people, locations and items such as weapons and vehicles) and may specify relationships among the entities they contain (e.g., person lives at address, or person owns vehicle). Although N-DEx will have the ability to process unstructured data, the majority of data supplied to N-DEx will be structured. N-DEx information services correlate data received from data suppliers and apply sophisticated business rules which may proactively notify specific users if certain relationships are discovered. N-DEx will prepare the data for efficient access through N-DEx services and capabilities to address the who, what, when, where and how of law enforcement information nationwide. It will also provide users with a single point of discovery to "connect the dots" through the N-DEx capabilities. In doing this, N-DEx will maintain knowledge of entities contained in data available to N-DEx in such a way that N-DEx will always know the relationships between a specific entity and its related entities even if that specific entity appears in multiple pieces of data from multiple data sources.

N-DEx users are offered access to the information available using the N-DEx capabilities. These capabilities provide the investigative and analytical tools for users to discover information across jurisdictional boundaries, relevant to their fight against crime and terrorism. For example, when a user conducts a search for a name, the system will automatically link and make available to the user, correlations between people, places, and things that previously were not known to the user.

The following sections describe the concepts for LEAs to access N-DEx services, capabilities and information for agencies acting as data sources to share data with N-DEx.

8 N-DEx Integration & Connectivity

N-DEx will perform a major central integration of today's complex and fragmented environment of many existing systems and information sharing efforts—often with varying methods of connectivity, authorization and data representation. Achieving this outcome will be a long-term journey requiring significant effort on the part of local, state, tribal, and federal LEAs. In recognition of this reality, a range of integration options are necessary to allow each participating LEA to choose an option that best fits its needs, size and budget. An agency may integrate in any of these ways, all of these ways, or in any combination. See Section 8.2 below for examples of integration options.

This section focuses on the nature of integration centering on two distinct purposes for integrating:

- Data integration where a LEA chooses a method to integrate its source system(s) commensurate with their state policy and supply the N-DEx community with data.

- Functional integration where a participating N-DEx user can connect to and use the capabilities and information provided by N-DEx.

8.1 Data Integration

The purpose of this section is to discuss incorporating or making available, data to N-DEx that is necessary to support N-DEx services and capabilities.

It is envisioned that, over time, criminal justice information of many varieties (e.g., incident reports, case files, field investigation reports, booking and incarceration records, criminal histories) from numerous local, state, tribal and federal systems will be shared with N-DEx. (Further discussion on data sources for N-DEx can be found in Appendix C). In general, the data sources that will supply N-DEx with data can be categorized into three types of integration described and illustrated below:

- **Non-Interactive (Push) Data Sources** - Data from Non-Interactive Data Sources contain sufficient information necessary to support a review of the full record. This eliminates the need for N-DEx to pull from the data source in response to user requests, allowing a simpler type of integration. The downside is that much larger records must be transported to and stored by N-DEx. The majority of LEAs fall into this type whereby structured incident reports contained in their RMSs or other repositories will be submitted to N-DEx through various means.

- **Interactive (Push-Pull) Data Sources**- Interactive Data Sources are tightly integrated with N-DEx such that N-DEx is made aware of the data contained in the data source; however, it does not include information necessary to support viewing the full record. Rather, N-DEx can subsequently request a "pull" from the data source full records when requested by N-DEx capabilities. For example, a Fusion Center may push an "index" of information it contains and in some cases relationships among that information. N-DEx would request a "pull" information from the system as necessary to satisfy user actions.

- **Leveraged Data Sources** - Sources that do not proactively make N-DEx aware of the information they contain are Leveraged Data Sources. These include legacy transaction-based systems that must be queried to provide a response. Included among these are NCIC and III (via NCIC).

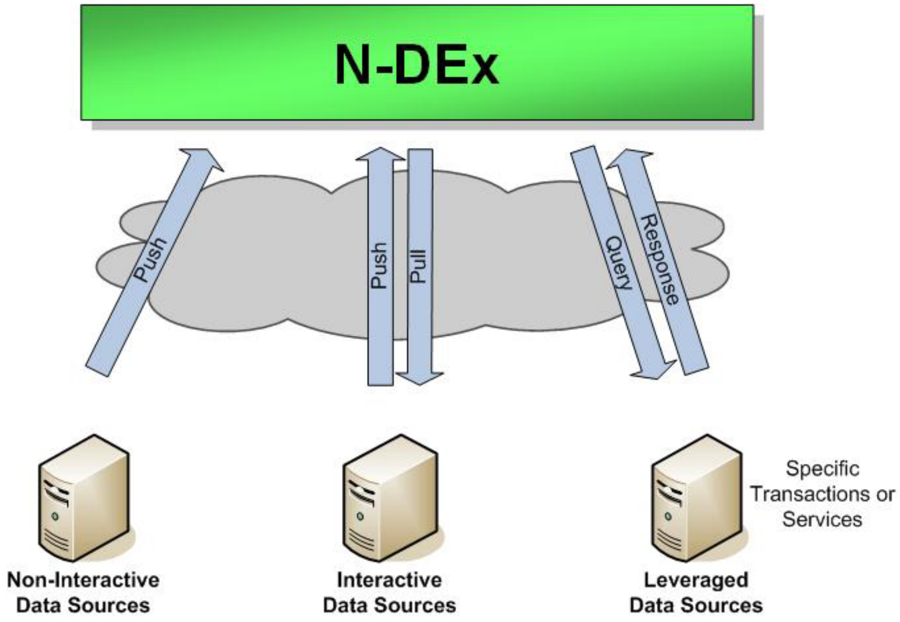


Figure 8-1. Data Source Integration

Numerous regional information sharing efforts in place today have already integrated data from regional systems, as well as state and local agencies. It is much more practical for these "repositories" to act as N-DEx data sources on behalf of the local agencies, than for each local agency to implement N-DEx-specific data source interfaces. This concept of federating the N-DEx data paths (e.g., locals to regions, regions to states and states to N-DEx) facilitates N-DEx. Ideally, N-DEx would obtain its data from 50 States' repositories working on behalf of the agencies within their states. However, this model of aggregation is not occurring nationwide. As such, N-DEx must be able to obtain its data through a variety of options as permitted by policy. Some LEAs will provide their data directly to N-DEx and others will provide it to repositories that will in-turn provide it to N-DEx. This is illustrated below for Non-interactive data sources.

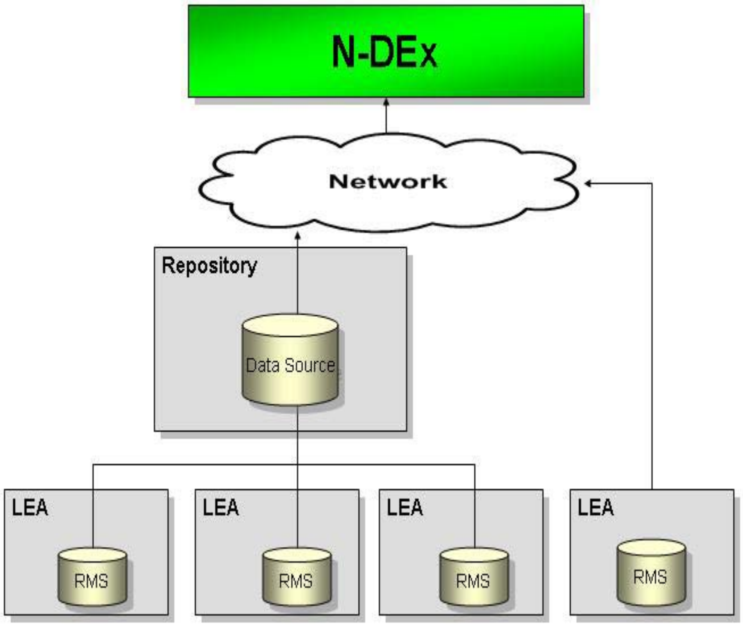


Figure 8-2. Non-Interactive Data Source Integration Examples

A major point for consideration is how the data are transported from the data source to N-DEx. Ideally, N-DEx will receive newly created records as soon as they are entered into data source systems. For example, a clerk enters an incident report in an LEA's RMS and it is immediately sent to N-DEx and made available for sharing in near-real-time. Additionally, N-DEx would be made aware of any changes (i.e., modify, update, delete) to that submitted record in near-real-time. Alternatively, data sources could submit data to N-DEx periodically in batch. Achieving widespread near-real-time integration described in the first example will not be realized overnight. N-DEx must accommodate the varying degrees of technical capabilities possessed by the data sources.

The following considerations also need to be addressed relative to data and integration:

- Only the data provider may change (add, delete, modify) data. To this point, data are only changed by submission from the source which owns them. N-DEx provides mechanisms to allow data sources to synchronize their data with N-DEx as data changes in their systems. N-DEx capabilities never allow modification of data; modification must originate from the providing source.

- The data owner has complete control over which N-DEx user roles have what kind of access to its data.

- A data POC is an N-DEx user who will be notified under specific conditions as part of specific N-DEx capabilities and information services relative to a specific data record/item. A default POC or group of POCs can be set for all records owned by a data source. Specific POC(s) can also be specified within individual records/items.

- N-DEx cannot assert the accuracy of information contained within its data supplied, or of the configuration delegated to data source administrators who are responsible for applying those mechanisms properly to their unique information.
- When a user search request correlates with information in a record, the user may wish to view the full information represented by the record. Assuming the user is authorized to view the full record, N-DEx will access it in one of two ways, depending on whether the data source is Interactive or Non-Interactive.

8.2 Functional Integration

The discussion in this section centers on functional integration types associated with users accessing capabilities, and information available through N-DEx. As depicted in Figure 8.3, N-DEx functionality can be accessed in two ways:

- **End-User Browser** - LEA users will be provided the ability to access N-DEx directly through a web browser (e.g., similar to accessing online banking or using an online auction).
- **Web Services** - All N-DEx user level capabilities will be available to external LEA systems through web service interfaces. For example, an agency system (e.g., case management or an RMS) or regional information sharing system may wish to integrate N-DEx capabilities into the local system's user interface. A user may be offered a national search option in this way. To perform that search request, the local system would send the request to N-DEx through web service interfaces and then incorporate the response from N-DEx into the local user interface visible to the end user.

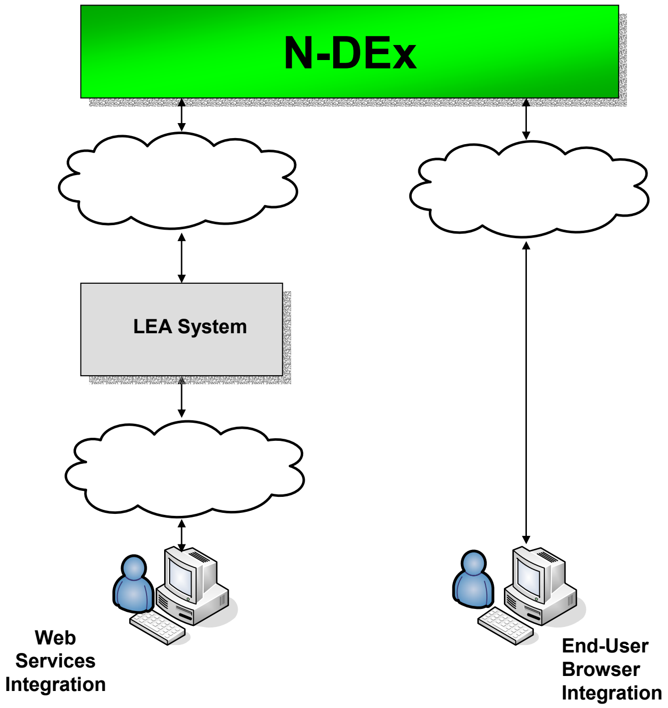


Figure 8-3. Functional Integration

8.3 Network Connectivity

CJIS will deliver N-DEx on the CJIS Wide Area Network (WAN). Connectivity to N-DEx from LEA systems and users will be through any means authorized in accordance with CJIS Advisory Policy Board (APB) policies and guidelines and in consultation with their state policy. Methods of connectivity may vary between LEA users connecting to the CJIS WAN from secondary locations. In many states, this will be accomplished through networks/systems that have long standing relationships with law enforcement nationally (Nlets, RISS.net, state networks, et.al.). LEAs will also be able to connect to N-DEx via secure Internet connections using the Law Enforcement Online (LEO) system. The CJIS WAN and the LEO system are the preferred methods for users and systems to connect to N-DEx.

9 System Characteristics/Requirements

This section discusses the system performance, sizing, quality factors, maintainability as well as general requirements with which the system must comply.

9.1 Performance and Effectiveness Factors

CJIS operates and maintains a number of very large systems containing millions of criminal justice records and information that is relied upon by local, state, tribal and federal criminal justice agencies nationwide. Among these are the NCIC and the III (See Appendix B for further discussion of these systems). NCIC averages nearly 4.8 million transactions daily with peaks reaching 5.6 million transactions per day while achieving an average response time of 0.06 seconds (for September 2005). NCIC service availability averages about 99.7% annually. This figure includes downtime for scheduled monthly maintenance. N-DEx is expected to be responsive to user service requests similar to that of NCIC.

It is envisioned that N-DEx will become a critical capability to the criminal justice community as other CJIS services have become. It is therefore expected that N-DEx be designed, implemented, operated, and maintained for high availability operations 24 hours a day, 7 days a week, achieving 99.5% operational availability or better. It is required that N-DEx be designed such that it is reliable; having no single points of failure and no loss of data. Within five years of N-DEx rollout, plans include a fully capable environment such that N-DEx could seamlessly provide its services following a catastrophic event resulting in devastation of the CJIS Data Center. These plans will however, depend on other CJIS disaster recovery efforts.

N-DEx should be designed, implemented, operated and maintained for ease of maintenance and require minimal downtime to be maintained, patched, or enhanced. Ideally, software and hardware maintenance will be performed without the need to take the system out of service.

N-DEx will provide system response times that are acceptable to users. It is highly desired that responses to user functions be as close to real-time as possible (e.g., within a few seconds) similar to response times achieved using Internet search engines over a broadband Internet connection.

9.2 System Sizing

This section describes the sizing and capacity needs of the system. It addresses capacities associated with data and users interacting with the system.

9.2.1 Data Capacities

N-DEx will establish a significant national repository of incident and case data as well as collect other types of criminal justice information such as incarceration and booking records, etc. Much of this data is currently collected in RMSs and repositories of the approximately 18,000 criminal justice agencies that exist nationwide. Though much of the Nation's LEAs collect incident-based data, the majority of crimes reported to the UCR Program are summarized into quantities of eight categories of crimes (UCR Summary) making it difficult to know the actual number of incidents. UCR data reported that in 2004, there were about 23.4 million offenses reported nationwide, 84% of which occurred in metropolitan areas.

Long-term plans are for N-DEx to collect, process, and make available for sharing the total of the Nation's incident data. Additional plans include the same for the Nation's incarceration and booking data as well as case data from a number of federal agencies to include the FBI. Other data will be added to the N-DEx repository or made available through N-DEx as possible.

The nature of law enforcement investigations is such that historical data may be equally important to solving crimes as is current data. Once N-DEx becomes operational, legacy data for the past five years will be gathered from participating agencies (where available) and placed in N-DEx to provide long-term value.

Ideally, data will be pushed to N-DEx from the Nation's repositories as soon as it is created in those repositories. Achieving this level of timeliness on a large scale may however take years depending on such factors as policy, model of integration, amount of data available, and technical capability. Until such time, N-DEx should expect to receive data in batches submitted at the agencies discretion (e.g., hourly, daily, weekly, monthly and randomly).

Privacy and security policies require retention of a variety of data including retention of what information has been disseminated to whom for the last five years. Operational drivers may increase data retention requirements significantly beyond five years.

9.2.2 User Capacities

N-DEx will become a common tool that is widely available to benefit all levels of law enforcement and criminal justice agencies nationwide. It is anticipated that N-DEx will be predominately used by investigators and analysts; however, N-DEx will have tactical use that could one day be deployed to patrol cars. In June 2000, the Bureau of Justice Statistics reported there were approximately 93,500 federal sworn personnel and 708,022 sworn state and local personnel. Although N-DEx will most likely not need to be made available to all sworn personnel, it must accommodate a significant amount of users through the various integration models described in Section 8.

9.3 Scalability and Flexibility

Scalability is a key consideration for a system that plans to share such a large and diverse amount of information to users nationwide. The long-term plans of N-DEx will not be realized overnight. It is therefore necessary that N-DEx grow commensurate with users' demands for data, number of users, functionality, performance, and funding availability. As the quantity of information available to N-DEx increases, enhanced levels of sophistication in search technology will become necessary to mitigate overwhelming users with non-relevant information.

N-DEx will be flexible to accommodate changes in functionality and information utilization as policy decisions are made and technologies mature during the life cycle of the system. For example, it is likely that demands for enhanced correlation and searching methods will increase as sources and quantity of data increase. Additionally, N-DEx flexibility will extend to incorporating new data types and data sources.

9.4 System Maintenance/Administration Concept

This section outlines important operation and maintenance (O&M) concepts and requirements for N-DEx once operational. A key consideration for N-DEx is that its life cycle maintenance be low cost. Considerations in this regard should be designed into this system.

O&M activities will initially be performed by the development contractor then transitioned to the CJIS O&M staff (FBI and contractor support) consistent with O&M for other CJIS systems.

9.4.1 System Administration

This section addresses system administration requirements for monitoring, system and application maintenance, problem detection/correction and backup and recovery.

9.4.1.1 Monitoring

The system will automatically monitor the current status of the system's applications and infrastructure and generate automatic notifications/alerts and/or warnings to the appropriate users so that they may proactively mitigate issues before they become problems. While most monitoring will be centralized to the CJIS Systems Management Center (SMC), other monitoring functions will be distributed and performed depending on the administrator's role. Monitoring will provide necessary information so that system administrators may:

- Ensure system availability, reliability, functionality, integrity, and efficiency
- Manage system resources such as performance, capacity, availability, serviceability, and recoverability
- Monitor all equipment supporting system and services
- Maintain event logs and reporting system/equipment availability
- Diagnose and resolve system problems and anomalies
- Provide centralized monitoring of critical processing points in the system
- Provide system performance monitoring, measurement, and tuning
- Ensure systems are maintained to meet availability and performance requirements
- Safeguard data integrity and monitor systems access to assure proper data usage and security

9.4.1.2 System and Application Maintenance

System Administrators will be responsible for ensuring that applications are functioning properly and updated. In addition to monitoring these applications and their supporting infrastructure, administrators will require a system that supports the automation of maintenance tasks, where possible, and provides robust interfaces in order to:

- Install, configure, troubleshoot, and maintain hardware and software

- Ensure system availability, functionality, integrity, and efficiency
- Install and integrate systems fixes, updates, and enhancements
- Startup and shutdown of the applications
- Design, plan, install, and implement system hardware and software upgrades

9.4.1.3 Problem Detection and Correction

The system will detect and correct minor problems and automatically report the problem, the resolution, and the current status to a System Administrator.

9.4.1.4 Backup and Recovery

The system will support backups and recovery of its data such that there is no potential for loss or corruption of data and no impact to user performance. CJIS Enterprise Storage Area Network (ESAN) and Integrated Backup infrastructure will be used to the extent possible.

Administrators will be responsible to monitor, performance tune, and provide backup and recovery of databases to assure their integrity. As part of this, they will schedule and verify system and database backups.

9.4.2 System Maintenance

System maintenance involves activities necessary to install and integrate hardware/software fixes, updates, patches, and enhancements to the existing system baseline.

The system will be placed under Configuration Management (CM) control and follow the CJIS Configuration Management Plan. All changes to the system baseline must be approved by the appropriate Technical Review Board(s) prior to change. A record will be maintained of all hardware/software versions, licenses, etc. All changes will be reflected in updates to the documented baseline.

9.4.3 Maintenance Support Environments

This section addresses the needs for development and test environment to support the maintenance of N-DEx through its life cycle. Key requirements of the environments will include:

- Provide environments segregated from the actual system and its data
- Allow the use of test data to include submission, modification and removal of test data
- Support multiple simultaneous development and test activities
- Ability to test new users/agencies that are coming on line
- Provide testing and data gathering tools

N-DEx will provide a Software Development Laboratory (SDL) environment dedicated to the development and maintenance of its system software. This environment will be used by multiple software developers to maintain and enhance the systems software baseline. The SDL needs to provide each developer a virtual environment to develop software and perform unit testing on that software.

N-DEx Non-operational Environment (NOE) will provide a test support environment to integrate and verify hardware and software capabilities and assess operational effectiveness and suitability. The N-DEx NOE will support testing of new or upgraded hardware, software and interfaces, and support end-to-end testing of N-DEx functions. This necessitates the NOE to be configurable to test the functionality, performance, quality factors and capabilities of N-DEx as well as N-DEx external interfaces. It needs to support the collection of data and statistics to verify the effectiveness of hardware and software configuration modifications and assist in analyzing anomalies and isolating faults. Additionally, the NOE will be used to support the maintenance of test procedures and documentation. To accomplish this, the test environment(s) need to cost effectively represent the operational environments as closely as possible. Also, the NOE needs to be capable of testing multiple baselines at the same time, such as the current system baseline and one or more future baselines (called builds).

The NOE will support testing for new agencies prior to their participation in N-DEx. The agencies will be able to submit test data or run tests and review the results. The system will also provide test reports for the users.

9.5 Security & Privacy

This section presents requirements and operational concepts for N-DEx system security which is focused on ensuring the integrity, confidentiality and availability of N-DEx's information and resources. This section also discusses the concept of privacy through authorization; enabling information sharing among law enforcement while establishing a secure, trustworthy environment to protect potentially sensitive information from unauthorized access.

The CJIS APB Security policies and the CJIS Controlled Access Protection Profile (CJISCAPP) have been established laying the groundwork for security. N-DEx must comply with the CJIS Security Policy of the APB and the CJISCAPP

The CJIS APB Security Policy provides the minimum level of Information Technology (IT) security requirements determined acceptable for the transmission, processing, and storage of the Nation's criminal justice information systems data. The full application of these requirements are necessary in order to establish uniformity and consistency in safeguarding CJIS data which is accessed via networks throughout the local, state, tribal and federal user communities. The minimum security requirements set forth in this policy shall not infringe upon the authority of a CJIS Systems Agency or an Interface Agency to invoke a more stringent policy.

The CJISCAPP specifies functional and assurance requirements for CJIS Criminal Justice Systems. CJISCAPP is based on National Security Agency (NSA) Information System Security Organization (ISSO) Controlled Access Protection Profile (CAPP), and was augmented with DOJ and FBI organizational security polices. There are two key constraints on CJIS Criminal Justice Support Systems that are asserted through the CJISCAPP. First, CJIS Criminal Justice Support Systems must connect to and interact with the computer systems of external criminal justice organizations. Secondly, the assertion that CJIS Criminal Justice Support Systems shall not process classified information, only public criminal justice information or Unclassified criminal justice information protected by the privacy act, and are designated SBU.

In general, N-DEx security requires:

- Support an access policy that restricts access to functionality and information based on the identity of users and/or the groups to which they belong. User access to functionality and data is restricted by roles.

- Support ownership mechanisms that allow users to specify and control sharing of information by named individuals, or by defined groups of individuals, or by both.

- Provide controls to limit propagation of access rights. Only authorized users will be permitted to assign access permission to functionality and information for users. Employing authorized users to set access permissions provides a level of assurance that specific N-DEx functions and information are protected from unauthorized access.

- A System Security Administrator (SSA) can define additional roles and the functional accesses. Potentially, a user may be assigned more than one concurrent role.

- Support providing access on a Need-To-Know (NTK) basis. NTK is defined as the necessity to have access to, knowledge of, or possession of specific information or data to carry out official job duties. Users only have access to the functionality and information that pertain to their job function.

- Support the capability to audit information and system actions. Must have ability to track information to ensure that it is not disclosed to unauthorized sources or applications and provide the ability to follow and report on all data disseminations.

- Support unique identification of each user and association of that identity with all auditable actions taken by that individual.

- Support of controlled interfaces.

9.5.1 Authorization and Privacy

The goal of this section is to discuss the concept considerations for authorization, privacy and potential impact on data formats, data sources and user administration. This discussion is not intended to stipulate a design or technological solution.

9.5.1.1 Authorization and Privacy Concept

A critically important responsibility of N-DEx from a Privacy and Security perspective is ensuring that users only see information they are authorized to see and only have access to functionality that they are authorized to have. Such operations are performed in the context of an authenticated user known by N-DEx to have associated privileges. N-DEx is responsible for providing these mechanisms so that information is protected, ensuring privacy as well as trust in sharing. Additionally, N-DEx is responsible for providing auditing and tracking capabilities to confirm the proper functioning of those mechanisms. Conceptually the responsibility for establishing and maintaining N-DEx users is delegated to agencies, which sponsor the users.

A wide variety of information will be shared in N-DEx from many local, state, tribal and federal agencies - each with its own privacy laws and policies. For example, privacy and criminal records laws across the 50 States are different. What one state can share may be restricted by another. N-DEx must provide mechanisms that data sources can configure to ensure the exchange and maintenance of shareable information complies with their applicable privacy standards and legal requirements. For example, a data source may wish to configure rules on N-DEx specifying how information is shared for certain data. These rules may be based on, among other things, criminal offense type and entity role as in the example where a data source wishes to restrict sharing of the identifying information incident data for a rape victim. Whatever the mechanism, LEAs must be able to trust that the information they contribute can be shared in a way that does not violate their own standards or jeopardize their missions or their personnel.

When an N-DEx user search "hits" on information or attempts to access or view information by any means, N-DEx must determine what type of access that specific user has based on the configuration provided by the data owner. Making that determination is what N-DEx authorization is all about. If all information shared with N-DEx were accessible to all N-DEx users, authorization would be dramatically simplified. However, this would mean only information suitable for dissemination to all N-DEx users could be shared within N-DEx at all. This would greatly restrict the amount of information which could be shared.

N-DEx Authorization must consider the following:

- The Information Sharing (INSH) Subcommittee of the CJIS APB appointed a task force to discuss access to information (and its associated privacy concerns). The subcommittee has focused on defining the resulting system actions when a specific user "hits" on, or attempts access to a specific piece of data. The subcommittee envisioned three types of access to protect the investigative equities through control of dissemination as follows:
    - **Full Access (Green)** – If the owner of a data record (e.g., incident report, arrest report) has designated the record and its data elements to be fully disseminated, then all N-DEx users with the appropriate access authority will have access to the full record and all data elements within the record.
    - **Pointer-Based Access (Yellow)** – If the data record owner decides that access to a specific record or specific data elements should be restricted except under certain circumstances, then the data owner can designate the record (or data elements) to be conditionally disseminated using pointer-based sharing. With pointer-based sharing, any user that gets a "hit" on, or attempts access to a record (or data element) with this designation, will be provided with information on the designated record owner's information (i.e., the POC for the record) only. It is then the responsibility of the data requestor to contact the owner who will determine whether the record (or data element) can be shared. If so, N-DEx provides mechanisms so that the data owner can make accessible that information to a specific user or group of users as applicable.

  - **Restricted Access (Red)** – There will be circumstances where a data record or part of the record is so highly sensitive that the data owner completely restricts dissemination of the data or access to it and any knowledge of that record to a selected user or user group. The value of having the record in N-DEx is that the data owner can benefit from correlations made with other N-DEx records without compromising the information contained in the sensitive record. With restricted access, any "hits" against the restricted record will be known to the owner user/group while the owner of the other record that it hit against, will have no knowledge of the correlation.

Assumptions relevant to N-DEx authorization include:

- Information which is fully shared for one user may not be fully shared for another user. For example, data may be fully shared within an agency or task force but restricted to pointer-based sharing to all other users.

- Data sources must have control over access to their data and their content, in terms of specifying which N-DEx users should be allowed what kind of access.

- Specific elements of data may have different access assigned. For example, identifying information for a rape victim in an incident report may not be shared, while the remaining information can be shared.

- All access to information will be done in the context of a specific user.

- If a user is not authorized to view information, the user must also be prevented from seeing side-effects of that information. As an example, imagine two incidents are correlated because victim identifying information in both incident reports appears to refer to the same person. If a user who is not authorized to view victim information hits on one incident, the correlation to the other incident should not be visible to the user.

- Since it is not possible to anticipate all future policy requirements which could arise impacting authorization, N-DEx authorization must be designed for flexibility, to maximize the likelihood that future policy requirements can be accommodated via configuration rather than system modification.

- The Authorization solution must have minimal impact to both data source/provider systems and personnel. Requiring significant changes to existing systems or requiring large investments in personnel would not be feasible.

- N-DEx will maintain knowledge of users who have access to N-DEx. Each user will have an associated set of user roles, which determine what actions the user may take and to what information the user has access. Administration and maintenance of N-DEx users is delegated to external agencies participating in N-DEx.

9.5.1.2 User Roles

Every N-DEx user will have an associated list of roles. A "role" in N-DEx is used for making authorization decisions. For example, roles might be defined based on job function (e.g., investigator, patrol officer), region of the country, agency association, citizenship, security clearance or other job characteristics which would drive a specific need. Job functions and their names may differ across jurisdictions. Users should have access only to data/information of functions that they need in performance of their job. N-DEx will allow agencies to assign personnel specific roles and create new roles.

9.5.1.3 User Authorities

In order to use N-DEx, either directly through the N-DEx portal or indirectly through an integrated external system, a user must have an account setup with N-DEx. This account specifies how the user will be authenticated and the roles associated with the user.

The N-DEx program staff will not normally have direct knowledge of the specific users. Rather, external agencies will be authorized to administer N-DEx users. Those external agencies are then responsible for assigning roles to individual users and guaranteeing that the users meet the role criteria. We refer to these agencies as User Authorities. N-DEx will have trust relationships with User Authorities allowing them to vet specific users for specific roles.

Consideration should be given to administration requirements of User Authorities. In addition to assigning roles initially, the User Authority must keep its user list and associated roles current as individuals leave the organization or change job function.

9.5.2 User Authentication

User Authentication is the process of confirming that the user requesting service is really the individual associated with the account in the user directory. Every access to N-DEx will be done in the context of a specific user.

Simple stand-alone applications have traditionally handled user authentication by simply requiring the user to sign in with a user id and password. For certain situations (in accordance with CJIS CAPP) this may be acceptable, however, that approach alone is insufficient for N-DEx.

N-DEx user authentication must consider the following:

- Agencies sponsoring N-DEx users (User Authorities) may have strong authentication mechanisms in place. Examples of this include DOJ Public-Key Infrastructure (PKI), and agencies required to comply with Homeland Security Presidential Directive (HSPD)-12. In such cases, end users should be able to access N-DEx using their agency-issued credentials (e.g., hard token) in a seamless manner.

- N-DEx supports integration of external systems with N-DEx capabilities, allowing N-DEx information and capabilities to be accessed using the local agency system and tools. In this case, users must still be authenticated, so that N-DEx can ensure that the user only accesses authorized information, and so that all access to information can be logged. For example, an authentication of the system that is accessing N-DEx is not sufficient. The user must be authenticated.

- N-DEx authentication will participate and inter-operate with other authentication efforts which are underway but not complete (e.g., DOJ PKI, LEO PKI). N-DEx will be dependant on these efforts for providing strong authentication.

9.5.3 Logging and Auditing

Policy states that all agencies providing access to N-DEx shall establish an audit trail capable of monitoring successful and unsuccessful log on attempts, file access, type of transaction, and password changes. All audit trail files shall be protected to prevent unauthorized changes or destruction. N-DEx will provide mechanisms to facilitate meeting this requirement.

9.5.4 Threat Protection

Requirements for threat protection provide secure mechanisms to identify, monitor and respond to security threats. They also provide for continual protection for computing resources and information. CJISCAPP specifies security objectives, which are derived from organizational security policy, and directed toward threat protection. Some of these include providing:

- Encryption Requirement - All CJIS data transmitted through any public network segment or dial-up or Internet connection (does not include radio frequency transmissions) must meet the CJIS APB Security Policy requirement to protect the data with a minimum of 128 bit encryption. For any procurement or upgrade to a system after September 30, 2005, the cryptographic module employed to achieve encryption must have a Federal Information Processing Standard (FIPS) 140-2 Certificate, issued by the National Institute of Standards and Technology (NIST) or the Canadian government Communications Security Establishment (CSE) to insure that the cryptographic module has been implemented correctly.

- Firewall protection for all external network traffic and all vital security related traffic needs;

- Intrusion Detection and Prevention capability;

- Monitoring and alarming for security and privacy;

- Application security to detect and prevent application layer attacks not detectable by traditional firewall and packet filtering, and to securely interact with automated and user driven application access; and

- Virus detection, isolation, and removal.

9.5.5 Certification & Accreditation

The FBI requires its systems to be examined for security when received from the vendor and before being placed into use. This is accomplished through the FBI's Certification and Accreditation (C&A) process as defined in the FBI C&A Handbook.

- Certification is the comprehensive evaluation of technical and non-technical security features and other safeguards of an Information System (IS), made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

- Accreditation is the Principal Accrediting Authority (PAA)/Designated Accrediting Authority (DAA) decision to formally accept security responsibility for a system based on the implementation of an approved set of technical, managerial, and procedural safeguards. It is also a business decision based on cost, performance, and the business case, as well as the security risk.

The C&A process serves as a form of quality control and ensures critical decisions are made, using adequate security safeguards and applying acceptable risk. This process covers the entire life cycle of an IS and is dependent on defining and documenting the system to be accredited, testing the technical and operational security features, producing a risk assessment, defining the security management positions and personnel for the system, and advising senior management of the system's security posture. A significant part of the security risk assessment necessary to support C&A involves testing to attempt to penetrate the security countermeasures of the system by a source independent to the system developer.

9.6 Interfaces

This section addresses some known interfaces to internal (to the FBI) and external systems as well as user interfaces. This is not meant to be a complete list as N-DEx will be ever changing, thus necessitating additional interfaces to systems having value to N-DEx. (Concepts for integration with these systems are discussed in Section 8). A primary goal when interfacing to systems is to minimally impact those systems. There should be minimal, if no changes, to systems in order to interface with N-DEx.

9.6.1 External Systems

N-DEx will interface with local, state, tribal, and federal external RMSs and data repositories of varying size and technological sophistication nationwide. These systems will range from local three man police department RMSs, to regional information sharing systems collecting information for a number of local agencies to state systems collecting information for all agencies contained in the state.

9.6.2 Internal Systems

N-DEx will provide one of the first steps in integrating services provided by FBI systems across its enterprise. N-DEx will do this by interfacing with a number of FBI systems and incorporating the services they provide into N-DEx functionality.

9.6.2.1 NCIC/III

N-DEx will employ existing interface services to integrate NCIC and III information into its services and capabilities. These systems are further discussed in Appendix B.

9.6.2.2 R-DEx

The envisioned end state is for N-DEx and R-DEx to operate in concert as the central hub of a law enforcement information sharing environment. Even though N-DEx and R-DEx will work together to implement the functionality of this central hub, the goal is to make that distinction invisible to external integrating systems. The fact that portions of the internal functionality will be delivered by R-DEx, and other portions by N-DEx, is an internal issue which does not affect external integrating systems.

To avoid making the internal division of labor between N-DEx and R-DEx apparent externally, this ConOps describes the combined functionality. When the envisioned end state is achieved, it will be more accurate to think of N-DEx and R-DEx as interdependent subsystems of a greater whole. Specifically, the R-DEx project will focus on unstructured or full-text search capability. Investments in building world-class technology in that area will be made through the R-DEx project.

9.6.2.3 SENTINEL

When complete, SENTINEL will be the automated case management system for use by the FBI. The case file represents the primary information repository for analysis and reporting and is used for supporting investigative, intelligence, and administrative work. N-DEx will receive case information from SENTINEL and N-DEx will provide its services to SENTINEL for integration into SENTINEL user functionality.

9.6.2.4 UCR

N-DEx will extract NIBRS data from submitted incident data when requested by an agency, and will simply pass this data to UCR.

9.6.3 User Interface

The amount of information and functionality provided by N-DEx will require a rich user interface. The N-DEx interface must be intuitive and easy to use and require as little training as possible for common user functions made available to the law enforcement community. Use of commonly used Internet-based conventions will contribute significantly to ease of use. The user interface must be Section 508 compliant. Help functionality should be provided.

Initially, the N-DEx user interface will be limited to browser-based capability targeted to desktop users; however, the user interface will likely evolve to provide capability to users in the field, possibly through wireless mobile devices like handhelds or patrol cars.

9.7 Technical Standards/Requirements

This section addresses technical standards, architectural and development requirements associated with the development and implementation of N-DEx.

9.7.1 GJXDM and NIEM

Extensible Markup Language (XML) will be the structured language for describing information being sent electronically to N-DEx. The GJXDM effort was organized under the leadership of the Office of Justice Programs, to explore and facilitate information sharing and technology integration in the justice and public safety communities. As part of this project, the Global Justice XML Data Dictionary (GJXDD) was developed. The latest version of GJXDD can be found at http://www.it.ojp.gov.

The N-DEx Program has developed an Information Exchange Package (IEP) using the GJXDM schema subset generator tool (http://www.it.ojp.gov). This IEP is ever evolving and the timeline for developing the next release will follow the release of GJXDM 3.1.0, June 2006.

The NIEM is using the GJXDM for building a common XML data exchange standard for information sharing among Department of Homeland Security (DHS), DOJ, and supporting communities in justice, public safety, homeland security, and intelligence.

The N-DEx Program will also develop an IEP using LEXS standards based on the latest NIEM release, located at http://www.niem.gov. In doing this, N-DEx will follow the guidance of the national standards bodies for development.

9.7.2 Commercial Off-the-Shelf

Commercial Off-the-Shelf (COTS) will be used in lieu of custom developed applications to the maximum extent possible. Choice of COTS will be the result of thorough evaluation. Any use of custom developed applications will be the result of analysis, reasoning, and engineering decisions.

9.7.3 Architectural

The paragraphs below address both the strategies and constraints that need to be considered architecturally.

9.7.3.1 Law Enforcement Information Sharing Program

The goal of the LEISP strategy is to enable DOJ to share law enforcement information with its local, state, tribal, and other federal partners and to facilitate multi-jurisdictional information sharing across the law enforcement and homeland security communities. The strategy formulates new DOJ law enforcement information sharing policies and business processes, and a Department-wide technology architecture aimed at confronting identified barriers to routine information exchange. When executed, the strategy will establish the Department as a committed partner in an information sharing environment of local, state, tribal, and other federal LEAs, where the power of information is marshaled to support their shared mission to prevent and prosecute terrorism and criminal activity. As N-DEx is an integral part of the LEISP strategy, it must be in alignment with the LEISP strategy.

9.7.3.2 Service Oriented Architecture

The N-DEx solution will conform to a Service Oriented Architecture (SOA). An SOA serves as a platform for gradual deployment of functional capabilities and common services that can be used by all FBI IT solutions. Simply stated, an SOA is a collection of services, or software agents, that communicate with each other. To ease communication between services, the SOA includes interfaces between each software agent, as well as an overarching plan that will allow new versions of software to be introduced without disrupting the existing systems. The SOA will enhance scalability, performance and reliability of the FBI's technical programs.

9.7.3.3 Federal Enterprise Architecture

As mandated in the Clinger Cohen Act of 1996, federal agencies must develop and maintain an enterprise IT architecture. By collaborating on cross-cutting activities, federal agencies can share staff efforts and products, thereby leveraging budget resources and lessening burdens. Collaboration can also encourage development of interoperability standards, which in turn, promote federal-wide information sharing and common capabilities. In serving the strategic needs and direction of this act, the Chief Information Officer (CIO) Council seeks to develop, maintain, and facilitate the implementation of the top-level enterprise architecture (EA) for the federal enterprise.

The Federal Enterprise Architecture (FEA) is a strategic information asset base that defines the business, information necessary to operate the business, technologies necessary to support the business operations, and transitional processes for implementing new technologies in response to the changing needs of the business.

The FEA Framework is a conceptual model that begins to define a documented and coordinated structure for cross-cutting businesses and design developments in the government. Collaboration among the agencies with a vested interest in a federal segment will result in increased efficiency and economies of scale. The FEA Framework promotes shared development for common federal processes interoperability, and sharing of information among federal agencies and other government entities.

The value of the FEA Framework is that it provides a mechanism for linking agency federal architecture activities, and promotes the development of quick successes within an overall federal architecture plan. This link allows agencies to work their architecture issues within the broader context of the FEA to reap the benefits of resource sharing and interoperability. Additionally, by allowing for quick successes, the model addresses real-world business needs of initiatives that provide strategic value.

N-DEx will conform to FEA guidelines in describing its solution.

9.7.3.4 CJIS Architecture

CJIS has developed a target architecture which consists of a set of products that portray the future or target state of the CJIS enterprise. The CJIS Target Architecture and the O&M environment necessitates that some products be standardized if the vendor chooses to use such categories of technologies provided by these products. A complete listing is available in the CJIS Target Architecture reference material.

Additionally CJIS has established enterprise solutions that N-DEx will leverage where possible as applicable. The CJIS ESAN and Integrated Tape Backup provides an enterprise solution to CJIS systems data storage that meet or exceed their anticipated CJIS data storage requirements for the next 3 to 5 years. Another enterprise solution is found in the FBI's LEO system. This system provides portal and collaboration capabilities such as e-mail messaging. Future plans are for LEO to become the enterprise authentication solution through HSPD-12 compliance.

9.7.3.5 Web Services

A web service is a collection of protocols and standards used for exchanging data between applications or systems. Software applications written in various programming languages and running on various platforms can use web services to exchange data over computer networks like the Internet in a manner similar to inter-process communication on a single computer. N-DEx will offer its services via web services and be capable of using services provided by other systems offering their services via web services.

9.7.3.6 Section 508 of the Rehabilitation Act

Section 508 of the Rehabilitation Act (29 U.S.C. 794d) requires that federal agencies' electronic and information technology is accessible to people with disabilities. N-DEx is responsible for compliance of Section 508 constraints at the server level only. There are specific restrictions designated by the Rehabilitation Act that include various limitations on color palettes, alternatives for hearing-impaired, alternatives for visually-impaired, alterations for physical limitations, and tactile differentiations.

9.7.4 Developmental Compliance Requirements

The development of N-DEx must be in concert with governmental requirements. This section describes some of the major directives, policies and laws that concern developmental compliance.

9.7.4.1 Records Management Division Certification

All new systems developed in the FBI require compliance through the Electronic Record Keeping Certification (ERKC), a process used to evaluate a system's compliance with records management criteria. The process is designed to guide system sponsors and developers in assessing and incorporating records management criteria into system requirement specifications, and then ensuring fulfillment through review of documented test results. The ERKC process consists of identifying systems that contain records, helping system owners and developers understand ERKC criteria, verifying specification of ERKC criteria through system requirements, and validating ERKC functionality through review of system test results.

Incorporation of this process at the earliest possible state in system development will minimize the effort required to meet ERKC requirements. Implementation of the ERKC process ensures that the systems developed and maintained by the FBI comply with statutory and agency requirements. The ERKC process incorporates record keeping in the system development life cycle so that all system development activities can appropriately consider record keeping issues from the earliest stages of acquisition and design.

9.7.4.2 System of Record Notification

Although data contributed to N-DEx will be controlled and maintained by the contributing agencies, the FBI's Records Management Division has determined that the N-DEx will be a system of records for purposes of the Privacy Act due to the records created through its correlations. Therefore, N-DEx must complete a Privacy Act Systems of Records Notice (PASRN).

The Privacy Act of 1974 (5 U.S.C 552a(e)(4)) requires publication of a notice in the Federal Register describing each system of records subject to the act. The publication requirements are intended to help individuals locate systems of records that are likely to contain personal information pertaining to them and prevent the use of a system or records without first giving individuals an opportunity to review the purpose and routine uses of the information.

Maintenance of a system of records for which no system notice has been published is a violation of the law.

9.7.4.3 Privacy Impact Assessment

The E-government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new information technology system because of the potential privacy impacts from maintenance of electronic databases. A Privacy Impact Assessment (PIA) is required to be conducted during the development and prior to the deployment of N-DEx.

A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. Personally identifiable information is defined as information in a system or online collection that directly identifies an individual. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. This involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project. The PIA process requires that candid and forthcoming communications occur between the program managers and the Privacy Office to ensure appropriate and timely handling of privacy concerns. This process also helps the public understand what information is being collected, how the information will be used or shared, how the information may be accessed, and how it will be stored.

9.7.4.4 Security Policy

As discussed in the Section 9.5, N-DEx must comply with the requirements of the CJISCAPP and the CJIS Security Policy of the APB.

9.7.4.5 Compliance with the NICS Brady Bill Legislation

If policy makers determine that N-DEx will use data provided by the National Instant Criminal Background Check System (NICS) on denial decisions, it must use this data in compliance with the Brady Handgun Violence Prevention Act (Brady Act) of 1993. Section 617 of Public Law 108-199, the Fiscal Year 2004 Consolidated Appropriations Act (or the Omnibus Bill), signed into law on January 23, 2004, requires that the NICS destroy any identifying information submitted by or on behalf of any person who has been determined **not** to be prohibited from possessing or receiving a firearm no more that 24 hours after the Federal Firearms Licensee (FFL) has been notified or the approval. The law provided that its record destruction requirement was to be implemented no later than July 21, 2004.

9.7.4.6 Life Cycle Management Directive

The FBI's IT Life Cycle Management Directive (LCMD) provides direction to each Program and Project Manager charged with the responsibility to manage programs and projects through their entire life cycle, from inception through deactivation. It sets the framework for development of thorough plans which, when executed with an appropriately tailored life cycle, will successfully deliver capabilities to FBI's user constituencies on schedule and within allocated budgets.

The IT LCMD is applicable to all FBI programs, projects, and personnel and is to be used by the Program and Project Manger to define programs and implement projects that will result in delivering high-quality IT systems to the FBI on time and within cost. As such, FBI Program and Project Managers will be held accountable for implementing the direction contained in this document. N-DEx will use the LCMD for its development, tailoring as necessary within the tailoring guidelines set forth in the LCMD.

9.7.4.7 CJIS QA

The CJIS Contract Administration Office's (CAO) Quality Assurance (QA) Program assists the CJIS Division in creating and maintaining the highest quality criminal justice IT systems possible, thus reducing criminal activity by improving response time and quality of the criminal justice information made available to the criminal justice community by the CJIS Division. The CAO QA Program will achieve this goal through continuous appraisal of CJIS IT systems in accordance with the FBI LCMD.

N-DEx will be developed in close coordination with CAO QA and the CJIS QA Plan which describes how the CAO QA Program will coordinate and administer quality assurance practices across CJIS to meet the mission of the Division. This QA Plan uses applicable DOJ and FBI policy, international and industry standards, federal regulations, and CAO objectives to implement QA throughout the CJIS Division.

9.7.4.8 CJIS CM

The CJIS CAO Configuration Management (CM) Program's goal is to ensure the security and integrity of the Division's information technology systems by identifying and maintaining control of their baselines. CM establishes and maintains consistency of a product's performance, functional, and physical attributes with the product's requirements, design, and operational information throughout the life cycle of the product.

N-DEx will be developed in close coordination with CAO CM and the CJIS CM Plan. This plan describes how the CAO CM Program will coordinate and administer configuration management practices across CJIS to meet the mission of the Division. The CM Plan follows the guidance of applicable DOJ and FBI policy, international and industry standards, federal regulations, and CAO objectives to implement CM throughout the CJIS Division.

10 Implementation

This section addresses the proposed approach for an incremental deployment of services and capabilities, the approach for prototyping and requirements/needs for training.

10.1 Acquisition Strategy

CJIS Division executive management, in consultation with the FBI and DOJ, have selected a performance-based acquisition strategy for N-DEx.

The performance-based approach differs from traditional government procurement where the contractor often is told exactly what to do, how to do it, what labor categories to provide, what minimum qualifications to meet and how many hours to work. In contrast, the performance-based approach focuses on the envisioned outcome. Under this approach, the N-DEx Program Management Office (PMO) will identify the problem to be solved in a Statement of Objectives (SOO). The responding bidders are asked to use their knowledge and experience to craft the best solution for designing and building the system. This will allow N-DEx managers to focus on achieving the vision as opposed to enforcing compliance with prescribed specifications.

10.2 Incremental Deployment

The complexities of implementation are significant, requiring an incremental deployment approach. This means the N-DEx services, capabilities and accessing options may not be delivered all at once. Initially, N-DEx will be developed to provide the services and capabilities per the priorities listed below. This will involve integrating N-DEx with CJIS services such as NCIC using existing interfaces provided by those systems. Although not included in the current concept, the potential exists for N-DEx to one day evolve to be the entry point (e.g., portal) to all of the services offered by CJIS providing users with a “one-stop-shopping” experience.

The performance-based acquisition will be a key driver to the approach for an incremental delivery based on a flexible component design that supports the scaling and adding of functionality along the development path. The acquisition needs to consider both the technical ramifications and the N-DEx priorities described below when recommending an incremental deployment approach.

Successful implementation will require an approach that addresses the diversity of the law enforcement community. Examples of this diversity include:

- **Privacy:** The Government’s design of and operation procedures for N-DEx will need to accommodate state and local privacy laws and policies, as well as the potential implications of state freedom of information acts on their information in some situations. The Government intends to take advantage of technology options for addressing privacy, but also realizes there may be practical limitations to doing so, including system “ease of use” issues and the capabilities of state and local systems that connect to N-DEx.

- **Data Availability:** The LEA data available for submission to N-DEx today spans a very broad spectrum, ranging from: LEAs with very sophisticated systems, databases and technology to those, generally smaller, LEAs, that have no automated data capabilities from which N-DEx submissions can be leveraged. For N-DEx to be successful, the

Government must accommodate the diversity of systems that could potentially provide data and develop data submission processes that are viable from an LEA operations perspective. N-DEx must do so in phases in order to address these issues in manageable increments. The N-DEx PMO is conducting a survey of state and local LEAs to gain a better understanding of the profiles today. The survey results will be available to contractors proposing an N-DEx solution.

- **Data Access Restrictions:** LEAs that contribute data to N-DEx will retain control of that data, and therefore will be able to determine access privileges to their data consistent with the overall policies and guidelines the CJIS APB establishes for N-DEx. The technical methods proposed to manage data access must take into account the practical limitations and operational procedures of the contributing LEAs. If the proposed solution is too onerous, many LEAs may limit their N-DEx submissions to only that data they can share unconditionally.

It is important to note that the order of completion of the desired changes may be affected by input from the development contractor to provide the most services and value in a logical order for design, development and implementation. The end state development of N-DEx is an overarching goal of the development process. Thus, the contractor's design should accommodate and anticipate growth in use and functionality.

All services and capabilities described under Section 5 are considered essential for complete functionality of the N-DEx system. It is anticipated that through the pending performance-based acquisition strategy the development will help set priorities and incremental deployment approach considering both the operational needs and the technical solutions.

The following are the operational priorities. To ensure initial success of the N-DEx system and demonstrate value early in the development/deployment process, these priorities should be considered for the first iteration of the N-DEx system.

- **Sharing of Incident/Case Report Information -** The N-DEx system must, at its foundation, create a platform where the ingestion of incident/case report information is possible and allow the sharing of this information among participating LEAs. This environment must comply with established constraints and assumptions iterated elsewhere in this document.

- **Search -** The N-DEx system must provide basic capabilities such as the ability to search data residing within the system. As it is anticipated that COTS will be used for this capability, the contractor should consider all capabilities associated with a search capability that these tools provide.

- **Correlation -** The following correlation services are desired in the following order:
  - Entity Correlation
  - Incident/Case Correlation
  - Entity Resolution

    - Automated Processing

- **Analytical/Reporting -** The capability to conduct in-depth analysis and to generate investigative reports from N-DEx data is a lower level priority but should be considered in the first iteration of the N-DEx system development.

10.3 Prototyping

In parallel with the development of N-DEx, a prototyping effort will be initiated to help refine national XML data standards and concepts, as well as provide near-term value to law enforcement. (For more details, reference the N-DEx Prototype Project Plan). This effort will present the strategic value of N-DEx to the user community while examining realistic user environments. The N-DEx design needs to take into consideration the feedback from operations of the deployment of a prototype system. The N-DEx PMO will work closely with LEAs to develop a prototyping plan, based upon:

- Existing, previous prototyping agencies and potential strategic value provided to N-DEx's development;

- Prototyping agencies' technical capabilities;

- Prototyping agencies' existing infrastructure; and

- Prototyping agencies' geographic location.

As a partner in prototyping, the selected LEAs will be requested to provide feedback on system services and their value. This feedback will maximize the value of outputs targeted in the full-scale system development.

Because one of the goals of prototyping is to determine the direction for N-DEx development, prototyping services and capabilities offered may differ from that of the final N-DEx system. In addition, the prototyping effort and the included functionality will cease once N-DEx becomes operational at which time prototyping agencies and contributed data will be transitioned to the N-DEx system.

11 Training

N-DEx users need a user friendly, online training environment that supports multiple roles including trainers and end users. The system will support initial system implementation training, new personnel assignment training, and recurrent annual training relating to all N-DEx business processes. It includes training for internal and external users, system administration/security, maintenance and operations personnel. Training will include development of User's Manual, Computer-Based Training, and Online Help.

11.1 Training Overview

The training environment will provide training capabilities for users accessing system training services remotely or locally at a CJIS facility. These components include a historical training database, online courses and a learning management system for managing training progress. (See *Figure 11-1* for a notional representation of the training environment). Users at designated CJIS training locations will be able to remotely access and operate selected N-DEx training modules. Remote users will have the option of choosing online training, downloadable courseware and documentation.

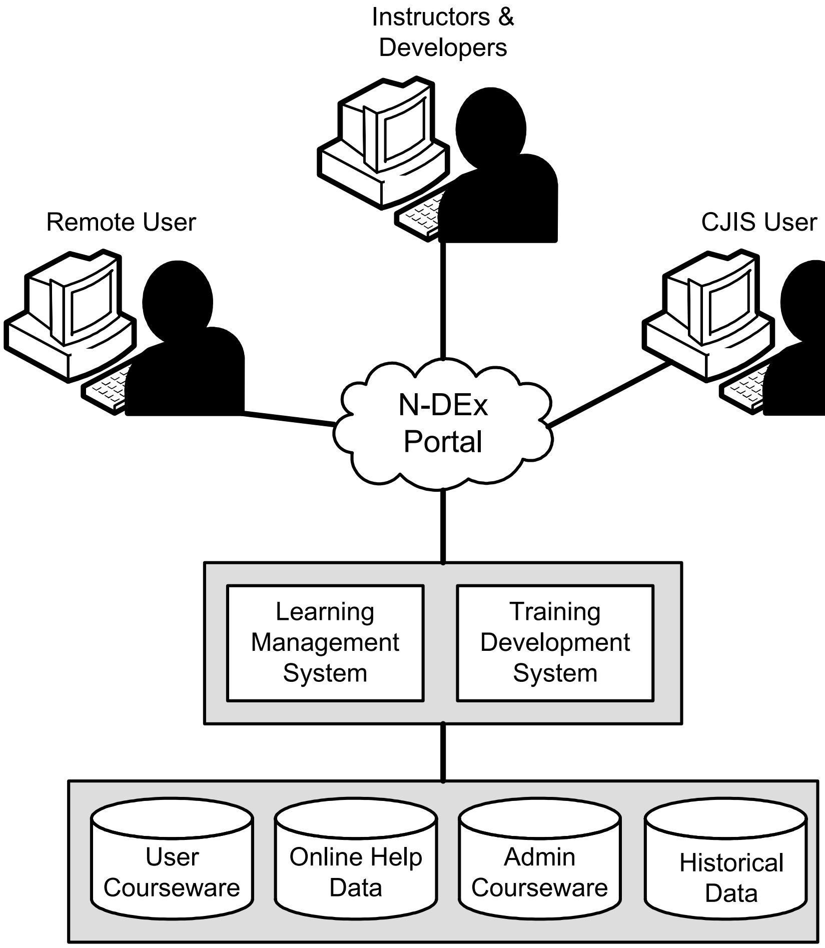


Figure 11-1. N-DEx Training Environment

N-DEx users will be provided learning management functions to include capabilities for training applications, historical data for training and a registration function for scheduling and tracking training progress. Access, scheduling, and registration in training courses may be made available from existing FBI Learning Management Systems if available and compatible with N-DEx. Training capabilities should include an environment where users may step through examples and practice use of the system functions using historical data.

N-DEx will also provide tools for development of either computer-based training or audio visual materials that communicate N-DEx capabilities. Candidates for training include N-DEx users such as law enforcement agents, as well as state and local administrators. N-DEx analysts and training developers will meet with FBI staff to coordinate the exact number and type of courses needed to deliver these training requirements.

11.2 Online Help

Daily system operations will be supported by online context sensitive and menu-driven help information. These system help files will provide the operator with detailed and indexed information on systems operations. Operators will have the capability to interrogate the help files while performing an N-DEx system interaction. The N-DEx system help files will suggest alternatives on how to navigate and operate standard N-DEx functions. Basic information about screens and options will also be provided.

11.3 Computer-Based Training

The training environment will make use of computer-based training (CBT) that enables users to go through examples, practice system functions and do exercises. These modules will be especially valuable to the remote N-DEx user who is unable to get to a CJIS classroom for instructor-led training. An off the shelf computer-based training and development tool as well as audio/visual resources will be made available to CJIS trainers to create new courseware, enhance existing training modules, and provide specific content in support of the N-DEx training functions.

11.4 Training Types

The N-DEx training function will be expandable for future training requirements. Training modules will be delivered in multi-media formats including compact disk (CD)(packaged audio/visual training for instructor or self-paced learning); electronically delivered CBT for self-paced learning, and as part of the N-DEx online help system. Online Training modules will provide both exercises and answers for hands on classroom training. Initial training materials will consist of:

- System Administrator Training - Overview of N-DEx system administration, recovery modes and general operations.
- System Security Administrator Training - Overview and documentation on N-DEx system security administration.
- N-DEx Application administration - Overview and documentation on the administrative procedures that include user creation, role and group assignment and access control.

- System Implementation Training - Overview of N-DEx, N-DEx components and procedure for installation and implementation.

- New Personnel Assignment Training—Overview of N-DEx, how to use the capabilities provided by N-DEx such as perform N-DEx searches, creating subscriptions, creating reports, and collaborating with users.

- Help Files - A set of online and indexed help files that describe user procedures, buttons, functions and user views, with related examples

- User Manual - An N-DEx user's manual covering the complete set of N-DEx capabilities will be provided.

Appendix A: Acronym List

AFOSI	Air Force Office of Special Investigations
APB	Advisory Policy Board
ARJIS	Automated Regional Justice Information System
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BCSO	Bailey County Sheriff's Office
BJA	Bureau of Justice Assistance
BOP	Bureau of Prisons
BTS	Border and Transportation Security
C&A	Certification and Accreditation
CAO	Contract Administration Office
CAPP	Controlled Access Protection Profile
CBT	Computer-Based Training
CD	Compact Disk
CJIS	Criminal Justice Information Services
CICJIS	Colorado Integrated Criminal Justice Information System
CIO	Chief Information Officer
CM	Configuration Management
ConOps	Concept of Operations
COTS	Commercial Off-the-Shelf
CSE	Communications Security Establishment
DAA	Designated Accrediting Authority
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
EA	Enterprise Architecture
ERKC	Electronic Record Keeping Certification
ESAN	Enterprise Storage Area Network
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FFL	Federal Firearm Licensee
GJXDD	Global Justice XML Data Dictionary
GJXDM	Global Justice XML Data Model
HPD	Henderson Police Department

HSPD	Homeland Security Presidential Directive
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Immigration and Customs Enforcement
IEP	Information Exchange Packet
III	Interstate Identification Index
INSH	Information Sharing (Subcommittee)
IP	Internet Protocol
IS	Information System
ISSO	Information Systems Security Organization
IT	Information Technology
ITN	Identification, Tasking and Network
JNET	Pennsylvania’s Justice Network
JTTF	Joint Terrorism Task Force
KCSD	Kent County Sheriff’s Department
LCMD	Life Cycle Management Directive
LEAs	Law Enforcement Agencies
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement Online
LESC	Law Enforcement Support Center
LEXS	Law Enforcement Information Sharing Program Exchange Specification
LInX	Law Enforcement Information Exchange
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
N-DEx	Law Enforcement National Data Exchange
NIBRS	National Incident-Based Reporting System
NICB	National Insurance Crime Bureau
NICS	National Instant Criminal Background Check System
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NJSP	New Jersey State Police
Nlets	The International Justice and Public Safety Information Sharing Network (formerly the National Law Enforcement Telecommunications System)
NOE	Non Operational Environment

NSA	National Security Agency
NTK	Need-To-Know
O&M	Operation and Maintenance
OAN	Owner Applied Number
ORI	Originating Agency Identifier
OSHA	Occupational Safety and Health Administration
PAA	Principal Accrediting Authority
PASRN	Privacy Act Systems of Record Notice
PIA	Privacy Impact Assessment
PIX	Proactive Information Exchange
PKI	Public-key Infrastructure
PMO	Program Management Office
POC	Point of Contact
PSP	Pennsylvania State Police
QA	Quality Assurance
RAIN	Regional Automated Information Network
R-DEx	Regional Data Exchange
RISS	Regional Information Sharing System
RMS	Records Management System
SBU	Sensitive but Unclassified
SDL	System Development Laboratory
SID	State Identification Number
SMC	Systems Management Center
SMS	Segment Management Server
SOA	Service Oriented Architecture
SOO	Statement of Objectives
SSA	Social Security Administration
SSAN	Social Security Account Number
TDPS	Texas Department of Public Safety
UCR	Uniform Crime Reporting
USMS	United States Marshals Service
VGTOF	Violent Gang and Terrorist Organization File
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

Appendix B: Current Systems

This appendix provides an expanded level of details from what was provided in Section 3.1.

B.1 FBI CJIS Division

The CJIS Division was established in February 1992 to serve as the focal point and central repository for criminal justice information services in the FBI. Located in Clarksburg, West Virginia, it is the largest Division within the FBI. The CJIS Division is responsible for the following: IAFIS, NCIC, UCR (to include NIBRS), NICS, and LEO.

The CJIS Division Mission:

Reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement related data.

B.1.1 Integrated Automated Fingerprint Identification System

The Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, is a national fingerprint and criminal history system maintained by the FBI CJIS Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. As a result of submitting fingerprints electronically, agencies receive electronic responses to criminal ten-print fingerprint submissions within two hours and within 24 hours for civil fingerprint submissions.

The IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for approximately 51 million subjects in the Criminal Master File. The fingerprints and corresponding criminal history information are submitted voluntarily by local, state, tribal, and federal LEAs.

IAFIS consists of three segments; the Automated Fingerprint Identification System (AFIS) segment, the Interstate Identification Index (III) segment, and the Identification, Tasking, and Networking (ITN) segment.

B.1.2 National Crime Information Center

NCIC is a nationwide information system dedicated to serving and supporting criminal justice agencies -- local, state, tribal, and federal -- in their mission to uphold the law and protect the public. Established in 1967, NCIC serves criminal justice agencies in all 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, and Canada, as well as federal agencies with law enforcement missions. NCIC provides a major upgrade to those services provided by NCIC and extends these services down to the patrol car and mobile officer. NCIC is a computerized database of criminal justice information that is available to virtually every LEA nationwide, 24 hours a day, 365 days a year, averaging 4.5 million transactions daily with peaks reaching 5.5 million per day.

The information maintained in NCIC assists authorized users in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. The NCIC database contains eighteen criminal justice data files. Eleven files contain information related to people while seven files contain information related to property. There is also a file for storing images and a file for agency information. The files included in NCIC are as follows:

Article File

< Records for any item having a unique manufacturer-assigned serial number (SER) and/or owner-applied number (OAN) valued at $500 or more; having a unique manufacturer-assigned SER and/or OAN, regardless of value, if aggregate value of all property taken in one theft exceeds $5,000; or any item having a unique manufacturer assigned SER and/or OAN, regardless of value, if interstate movement is indicated, or the stolen item is a lead in a more serious crime.

Boat File

< Records for stolen boats, boat trailers, or boat parts.

Deported Felon File

< Records for criminal aliens who have been deported for drug or firearms trafficking and/or serious violent crimes. The reentry of these criminal aliens into the U.S. violates Title 8, USC, Section 1326.

Foreign Fugitive File

< Records for persons wanted by another country for a crime that would be a felony if it were committed in the U.S. Wanting country must be a signatory to an extradition treaty or convention with the U.S.

Gun File

< Records for serially-numbered stolen weapons; recovered (abandoned, seized or found) weapons for which the owner is not known; or lost or missing weapons if the entering agency has supporting documentation.

License Plate File

< Records for uniquely-numbered stolen license plates.

Missing Person File

< Records for persons of any age who are missing and have proven physical/mental disability or are senile, missing under circumstances indicating that they may be in physical danger, missing under circumstances indicating that their disappearance may not have been voluntary, missing and declared unemancipated as defined by the laws of their state of residence and do not meet any of the above criteria, or missing after a catastrophe, or for persons over the age of 18 not meeting the criteria for entry in any other category who are missing and for whom there is a reasonable concern for their safety.

Originating Agency Identifier (ORI) File

< Records for agency information on any agency that has been assigned an NCIC ORI for the purpose of accessing the NCIC System.

Protection Order File

< Records of individuals who are subject to an injunction or any other order that restrains them from committing violent or threatening acts or harassment against another person, including temporary and final orders issued by civil or criminal courts.

Securities File

< Records for serially-numbered stolen, embezzled, used for ransom, or counterfeited securities, e.g., currency and documents or certificates that are considered evidence of debt or ownership of property, or documents that represent subscription rights. Also, warehouse receipts, traveler's checks, money orders, savings certificates, and interest coupons on stocks and bonds.

SENTRY

< Records for individuals incarcerated by the Bureau of Prisons.

Convicted Sexual Offender Registry File

< Records for the following subjects as per Title 42, USC, Section 14072(a): a person who has been convicted of a criminal offense against a minor, a person who has been convicted of a sexually violent offense, or a person who is a sexually violent predator.

Convicted Person on Supervised Release File

< Records for subjects that are under specific restrictions during their probation, parole, or supervised release following imprisonment.

Unidentified Person File

< Records for unidentified deceased persons, persons of any age who are living and unable to ascertain their identity, unidentified catastrophe victims, and body parts.

U.S. Secret Service Protective File

< Records for individuals who may pose a threat to the President and/or others afforded protection by the USSS as authorized by Title 18, USC, Section 3056 and Public Law 90-331 as amended.

Vehicle File

< Records for stolen vehicles, vehicles involved in the commission of a crime (felony vehicle), or stolen component parts.

Vehicle/Boat Part File

< Records for serially-numbered stolen vehicle/boat parts.

Violent Gang and Terrorist Organization File (VGTOF)

< Records for violent gangs and their members.

< Records for terrorist organizations and their members.

Wanted Person File

< Records for individuals (including juveniles who will be tried as adults) for whom a federal warrant is outstanding or for whom a felony or serious misdemeanor warrant is outstanding, and probation and parole violators.

< Records for juvenile offenders may be entered for escapees, probation and parole absconders, and for those juveniles charged with the commission of an act of delinquency that would be a crime if committed by an adult and who have fled from the state in which the act was committed.

< A temporary felony want may be entered when a law enforcement agency must take prompt action to apprehend a person (including a juvenile) who has committed, or there are reasonable grounds to believe has committed, a felony and may flee across jurisdictional boundaries and a warrant cannot immediately be obtained.

In addition, NCIC also acts as an interface to other systems and information by providing specific message-based query access. Some of the systems available by way of NCIC include: III and the ICE Law Enforcement Support Center (LESC).

B.1.3 Interstate Identification Index

A segment of IAFIS, III is the holder of the descriptive information links to criminal history associated with the criminal subjects housed in approximately 51 million criminal history records. Some of III's records are maintained at CJIS while others are distributed among a number of state systems.

Criminal justice agencies query III via NCIC using identification descriptors to determine if a subject of interest has a criminal record. When a record is found, III responds with summary information containing the subject's FBI number and/or State Identification Number (SID). An interested law enforcement user may then electronically request and retrieve the criminal history record by submitting a second NCIC request with the assigned FBI or SID number.

The existence of an FBI number in III indicates that a record is maintained by the FBI. Such records typically contain information concerning federal or foreign offenders, persons arrested in non-III states, the District of Columbia or U.S. Territories, and criminal arrests that III states are unable to provide.

The existence of an SID number or multiple SID numbers indicates that a record is maintained by one or more of the 48 III participating State Bureaus. When requested, these records are provided by the responsible State Bureau and contain as much, or often more, detailed information than the FBI records.

III also provides additional identifiers (aliases, additional dates of birth, miscellaneous numbers, etc.) from it's index. Since the search is name-based, III may find and return multiple FBI numbers and/or SID numbers for several people with similar names and dates of birth. For this reason, agencies using III must use professional judgment when associating records with individuals based solely on names and descriptors. A positive identification can only be made by fingerprint comparison. All III records have associated fingerprints.

B.1.4 Law Enforcement Support Center

Although LESC is not a part of CJIS, it plays an important role in the services provided through CJIS. ICE is a component agency of the Border and Transportation Security (BTS) and the DHS. The ICE mission is to prevent acts of terrorism by targeting the people, money and materials that support terrorist and criminal activities. A useful tool for achieving the ICE mission is provided by LESC. LESC supplies authorized law enforcement with information on aliens suspected of criminal activities and the status information of aliens under arrest. LESC is queried through NCIC via electronic messages that are passed to LESC via the International Justice and Public Safety Information Sharing Network (formerly the National Law Enforcement Telecommunications System), or Nlets. An LESC response is not an immediate response. Average response time is 20 minutes due to human intervention that takes place at LESC.

B.1.5 Uniform Crime Reporting Program

The UCR Program was conceived in the 1920s when the International Association of Chiefs of Police (IACP) envisioned the need for statistics on crime in the Nation. The Committee on Uniform Crime Records of the IACP developed the national collection effort in 1930 and in August 1930 the FBI assumed oversight of the UCR Program. This program compiles and publishes data submitted voluntarily by over 17,000 local, state, tribal, and federal LEAs. The UCR Program has served as a means of measuring crime in the United States since 1930. Currently, the FBI collects UCR data in two forms: the original hierarchical Summary method and the NIBRS method. The significant difference between NIBRS and the traditional Summary reporting system is the degree of detail in reporting. The Summary method includes only aggregate totals collected on eight Part 1 crimes. NIBRS is an incident-based system designed to collect data on each single incident and arrest within 22 offense categories made up of 46 specific crimes called Group A offenses. In addition to the Group A offenses, there are 11 Group B offense categories for which only arrest data are collected.

B.1.6 National Instant Criminal Background Check System

The Brady Handgun Violence Prevention Act of 1993 required the Attorney General to establish the NICS in November 1998. NICS conducts background checks for FFLs; reviews records to determine whether or not the prospective purchaser is specifically prohibited from receiving a firearm; and processes appeals resulting from denials of firearms background checks. NICS averages eight million processed transactions a year and has approximately 490,000 denials on record (as of March 31, 2006). Data in NICS are not used to establish a federal firearm registry. Information which resulted in an allowed transfer is destroyed. Data extracted pertaining to denial decisions are forwarded to the Bureau of Alcohol, Tobacco, Firearms, and Explosives as the regulatory agency. *(N-DEx will only utilize the Denial Decision Extract File.)*

B.1.7 Law Enforcement Online

LEO is a 24 hours a day, 7 days a week (24 X 7) on-line (real-time), controlled-access communications and information sharing data repository. It provides an Internet accessible focal point for electronic SBU communication and information sharing for the local, state, tribal, and federal LEAs. LEO also supports anti-terrorism, intelligence, law enforcement, criminal justice, and public safety communities nationwide. Users anywhere in the world can communicate securely using LEO. LEO is accessed by vetted and authorized entities using industry-standard personal computers equipped with any standard Internet browser software, along with LEO supplied Virtual Private Network (VPN) encryption software. LEO currently supports a user base of over 36,000 individual users, who access LEO either via the Internet, dialup, or other dedicated connections. In addition to the current LEO user base, there are 17,000 Regional Information Sharing Systems (RISS) users that have the ability to access LEO. LEO currently has 1,200 RISS users. LEO operates as a SBU network under the Computer Security and Privacy Acts. In summary, LEO provides a mechanism for law enforcement entities to share data internally and externally.

B.2 Local/Tribal

More than 18,000 LEAs make up the front line of the Nation's defense against crime and terrorism. These agencies use a multiplicity of systems and system types for records management purposes (ranging from high end computerized systems to paper-based systems). Follows is one example of a computerized system being used by a local agency.

Los Angeles County: The first system that used a middleware approach was the Los Angeles Proactive Information Exchange (PIX) system. This system, first implemented in 1989, gradually brought individual agencies online. Designers knew they would never get all criminal justice agencies to agree on one common database so they sought a central middleware solution like PIX that would allow each agency to determine what data they would give to other agencies. PIX allowed each agency to determine what data they would send to other agencies and when they would send the information. The high cost of replacing existing systems also influenced their design decisions.

B.3 Regional

Many regional models have demonstrated the value of combining resources including information and jurisdictions for special purposes (e.g., task forces separately targeting drugs, gangs, organized crime, fraud).

R-DEx: The Regional Data Exchange (R-DEx) System is an FBI partnership initiative with a range of evolving regional information sharing initiatives that is building a data repository of unstructured criminal justice information. R-DEx serves as the first implementation of the "One DOJ" principle contained in the LEISP strategy. That principle commits DOJ to quickly share law enforcement information from all DOJ components with local, state, and tribal law enforcement. The goal is to enable DOJ to join participating local, state, tribal, and federal LEAs in regional full-text information sharing under standard technical procedures and policy agreements. The information contained on this system consists of SBU criminal law enforcement records collected and produced by the following DOJ components: the Federal Bureau of Prisons (BOP); the United States Marshals Service (USMS); field offices at the ATF, the DEA, and the FBI. Initially, R-DEx information will be shared with participants of two regional information sharing initiatives, the Law Enforcement Information Exchange (LInX) and Gateway (see below).

LInX – a regional sharing initiative based in Seattle, Washington. The LInX System provides access to law enforcement incident and investigative data collected and contained within a regionally centrally located data warehouse. The LInX System leveraged the previously established Regional Automated Information Network (RAIN) system developed by the King County Sheriff's Office.

Gateway - an information sharing initiative in the St. Louis, Missouri area. Data submitted is full text with search and linkage analysis capabilities. Agencies participating in Gateway includes: St. Louis Metropolitan Police Department, St. Louis County Police Department, Illinois State Police, Missouri State Highway Patrol, St. Clair County Sheriff's Office, and the FBI St. Louis Division.

San Diego County: The Automated Regional Justice Information System (ARJIS) is a complex criminal justice enterprise network utilized by 50 local, state and federal agencies in the San Diego region. ARJIS is chartered with supporting a regional web-based enterprise network that utilizes technical and operational standards to build interfaces to all criminal justice systems in the region. The ARJISNet secure intranet contains data on the regions crime cases, arrests, citations, field interviews, traffic accidents, fraudulent documents, photographs, gang information and stolen property. ARJISNet integrates over 2,500 workstations and printers throughout the 4,265 square miles of San Diego County. There are over 10,000 registered and authorized users generating over 35,000 transactions daily.

B.4 Fusion Centers

Fusion Centers are a central conduit for information sharing among numerous LEAs in a particular region.

RISS: The RISS Program is an established system of six regional centers (e.g., Northeast, Middle Atlantic-Great Lakes, Southeast/Southwest, Rock Mountains, and Western) that are used to share information and coordinate efforts against criminal networks that operate across jurisdictional lines. The RISS Program was created to the mid-1970s to combat traditional law enforcement targets, such as drug trafficking and violent crime, but was expanded post 9/11 to include other activities, such as terrorism and cyber-crime. The RISS program uses a regional approach, so that each center can tailor/focus its resources on the specific needs of its area, while still coordinating and sharing information as one body for national-scope issues. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber-crime, gang activity, and organized criminal activities. Each of the centers, however, selects its own target crimes and the range of services provided to member agencies. The vast majority of member agencies are at the municipal and county levels, but state and federal agencies are also members. Federal agency members include DEA, FBI, U.S. Attorneys', Internal Revenue Service, U.S. Secret Service, ICE, and ATF.

B.5 State

Many states have recognized the need to share information across jurisdictional boundaries and have implemented state-wide programs to accomplish this information sharing.

Colorado: The Colorado Integrated Criminal Justice Information System (CICJIS) uses the middleware approach to systems integration. The system is shared by prosecution, courts, probation and law enforcement. The system was mandated and funded by the Colorado legislature in 1995 and system design began in 1996. From the beginning, one of the main goals of the system was to keep autonomous agency systems intact but enable communication between systems in such a way as to create one unified virtual system. In order for this to happen, all agencies had to agree upon one unique defendant identifier that would be used as a primary medium of exchange. The identifier selected was the SID. This number is a fingerprint-indexed number assigned to defendants at their first arrest and kept by defendants for the remainder of their lives. Each time a defendant is re-arrested he or she is linked to the SID number.

Pennsylvania: Pennsylvania's Justice Network (JNET) is an example of a virtual system. JNET is a statewide integrated system that emphasizes timely criminal history and court information. This system was mandated in 1996 by executive order of the Pennsylvania governor with the dual goals of improving operating efficiencies and enhancing public safety. What is unique about JNET is that it is being implemented as an Internet browser-based system running on a state-operated Intranet.

Appendix C: N-DEx Data

The intent of the following section is to illustrate the range of potential data sources that may be available to N-DEx. This listing continues to be In Work status (especially the latter portions). Follows is a skeleton of potential items that will exist within the Appendix (once completed) and within the N-DEx System.

C.1 Incident Report

Incident reports are used nationwide to collect, record and report law enforcement incidents related to criminal offenses. These reports are comprised of specific identifying data (names of suspects/victims/witnesses, locations, addresses, vehicles, weapons, etc.) and nonspecific descriptive data (offense, method of entry, victim data, offender data, relationships such as victim to offender, et.al.). Incident reports include the who, what, when, where, and how of the activity that occurred. In some jurisdictions, incident reports are followed by investigative reports, case reports, or supplemental reports that contain additional or follow-up information to the original incident report.

C.1.1 Value

The incident report data would be used to build an information repository of people, places and things for searching and will also provide the information needed for identifying relationships, crime characteristics or modus operandi to link incidents or cases together. Additionally, this data would be used to analyze crime trends for law enforcement response.

C.1.2 Data Source Provider(s)

Incident reports are captured and maintained throughout the nation by the individual local, state, tribal, and federal LEAs that respond to and investigate incidents and calls for service occurring within their specific jurisdiction. In some states, regional and/or state centralized databases also capture and maintain these records.

C.1.3 Data Availability

Incident reports captured and maintained by the individual LEAs are housed in a wide variety of formats. The method used to maintain these records range from paper formats to sophisticated electronic systems. Electronic records management systems used by individual LEAs as well as regional and/or state centralized databases also vary from internally developed systems to purchased vendor software.

C.2 Arrest/Booking Data

Arrest data is normally collected by individual LEAs in relation to actions taken to cite, arrest, incarcerate, or otherwise substantially deprive an individual of his/her normal civil liberties. Booking data is normally collected after the arrested person is brought to the law enforcement office, which involves the recording of the person’s name, the crime for which the arrest was made, and which may also include photographing, fingerprinting, et.al.

C.2.1 Value

Arrest/Booking reports would provide specific identifiers and possibly photographs of subjects for searching and would also provide the information needed to link individuals, incidents or cases together. Additionally, this data would provide a location of a subject at a specific time.

C.2.2 Data Source Provider(s)

Arrest/Booking reports are normally captured and maintained throughout the nation by the individual local, state, tribal, and federal LEAs. Incarceration facilities also may capture and maintain this data. In some states, regional and/or state centralized databases may also capture and maintain these records. The Joint Automated Booking System (JABS) is the centralized system that captures and maintains federal booking data.

C.2.3 Data Availability

Arrest/Booking reports are captured and maintained by the individual LEAs and are housed in a wide variety of formats. The method used to maintain these records range from paper formats to sophisticated electronic systems. Electronic records management systems used by individual LEAs as well as regional and/or state centralized databases also vary from internally developed systems to purchased vendor software.

C.3 Incarceration Records

Incarceration data collected by LEAs details the confinement of an individual in a local jail or state/federal penitentiary. This data includes specific identifying data, which may include photographs of individuals, fingerprints, et.al. of subjects that have been incarcerated.

C.3.1 Value

Incarceration records would provide more detailed and accurate specific identifying data. For example, a subject may provide a false address or personal identifier at the time of arrest. Upon conviction and sentencing, or when incarceration is imminent, the same subject may provide different (possibly more accurate and truthful) information such as address, date of birth, et.al. Incarceration data would provide a location of a subject at a specific time and could also provide known associates to a subject in the form of visitor logs, cell mates, and other information regularly captured by incarceration facilities.

C.3.2 Data Source Provider(s)

A state Department of Corrections typically captures and maintains data from the state incarceration facilities into a centralized database. Local jail facilities are normally operated on the county Sheriff level and the data is captured and maintained throughout the nation by these individual local agencies. In rare instances, regional and/or a state centralized database capture and maintain these local facility records. The Federal Bureau of Prisons maintains the SENTRY system which is a centralized system that captures and maintains Federal incarceration data. Some incarceration data may be maintained by private or contracted companies working with local or state jurisdictions to provide incarceration services.

C.3.3 Data Availability

Incarceration data captured and maintained by the incarceration facilities are housed in a wide variety of formats. The method used to maintain these records range from paper formats to sophisticated electronic systems. Electronic records management systems used by incarceration facilities and regional and/or state centralized incarceration databases also vary from internally developed systems to purchased vendor software.

C.4 Probation Records

Probation records are normally collected by LEAs or Judicial Agencies involved with the suspension of imprisonment for an offense where future punishment looms should the individual choose not to comply with his/her conditions of supervision. These reports are comprised of specific identifying data and include the conditions to which a subject must abide.

C.4.1 Value

Probation records would provide specific identifiers and possibly photographs of subjects for searching and would provide the information needed to link individuals, incidents or cases together. Additionally, this data would provide a location of a subject at a specific time and could also provide known associates to a subject in the form of employment data, et.al. The probation conditions to which a subject must abide would be readily available to LEAs.

C.4.2 Data Source Provider(s)

Probation records are captured and maintained throughout the nation by the various agencies that are involved with the initial placement and monitoring of the individuals placed on probation in their specific jurisdiction. Law enforcement agencies, Judicial Agencies, and agencies under private contract are examples of the range of entities collecting this data. In some states, regional and/or state centralized databases also capture and maintain these records.

C.4.3 Data Availability

Probation records captured and maintained by these agencies are housed in a wide variety of formats. The method used to maintain these records range from paper formats to sophisticated electronic systems. Electronic records management systems used by individual LEAs as well as regional and/or state centralized databases also vary from internally developed systems to purchased vendor software.

C.5 Parole Records

Parole records are normally collected by LEAs or Judicial Agencies involved with the early release of an offender from imprisonment, depending upon his/her acceptance of and compliance with a set of conditions. These reports are comprised of specific identifying data and include the conditions to which a subject must abide.

C.5.1 Value

Parole records would provide specific identifiers and possibly photographs of subjects for searching and would provide the information needed to link individuals, incidents or cases together. Additionally, this data would provide a location of a subject at a specific time and could also provide known associates to a subject in the form of employment data, et.al. The parole conditions to which a subject must abide would be readily available to LEAs.

C.5.2 Data Source Provider(s)

Parole records are captured and maintained throughout the nation by the individual LEAs or Judicial Agencies that are involved with the initial placement and monitoring of the individuals placed on parole in their specific jurisdiction. In some states, regional and/or state centralized databases also capture and maintain these records. Additionally, some states' Department of Corrections capture and maintain this data.

C.5.3 Data Availability

Parole records captured and maintained by the individual LEAs are housed in a wide variety of formats. The method used to maintain these records range from paper formats to sophisticated electronic systems. Electronic records management systems used by individual LEAs as well as regional and/or state centralized databases also vary from internally developed systems to purchased vendor software.

C.6 NCIC

The NCIC database contains eighteen criminal justice data files. Eleven files contain information related to people while seven files contain information related to property. A complete description of the NCIC files is provided in Appendix B.

C.6.1 Value

NCIC data would assist authorized users in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. For example, every name included in a standard incident report recorded by an LEA is not always queried through NCIC. Fugitives may not have been queried through NCIC that were listed as a victim or witness on an incident report. N-DEx would have the ability to conduct an NCIC query on all names recorded on a submitted incident report.

C.6.2 Data Source Provider(s)

NCIC data is a computerized index of documented criminal justice information submitted by local, state, tribal, and federal law enforcement agencies nationwide.

C.6.3 Data Availability

NCIC is a legacy transaction-based system maintained by the FBI CJIS Division.

C.7 III

III is a segment of IAFIS and houses approximately 51 million criminal history records. In addition to disposition data, III also contains physical descriptors, and the identity of the data base(s) maintaining state bureau criminal history record information. A complete description of III is provided in Appendix B.

C.7.1 Value

III data would provide specific identifiers and possibly photographs of subjects for searching and would also provide the information needed to link individuals, incidents or cases together. Additionally, the disposition data would provide a location of a subject at a specific time.

C.7.2 Data Source Provider(s)

III data is a computerized index of documented criminal justice information submitted by local, state, tribal, and federal LEAs nationwide.

C.7.3 Data Availability

III is a legacy transaction-based system maintained by the FBI CJIS Division.

C.8 Federal Firearms Licensee Data

FFL data would provide access to individuals that possess a Federal Firearms License.

This data would provide descriptive identifiers for the FFL and could be used for tactical planning.

C.9 Pawn Shop Ticket

Pawn Shop transaction ticket information could be very beneficial to LEAs. A Pawn Shop transaction requires proper form of identification and a detailed explanation of the goods being pawned (description of a piece of electronic equipment, must include the year of manufacture, model, serial number, et.al.).

This data would provide descriptive information on possible stolen items and descriptive identifiers of the pledgor.

C.10 Immigration and Customs Enforcement Data

The ICE Data provides a wide range of informational services to N-DEx. It is the single national point of contact that provides timely immigration status and identity information on aliens suspected, arrested, or convicted of criminal activity.

This data would provide immigration status for LEAs.

Appendix D: Referenced Documents

This appendix contains the referenced documents contain in the N-DEx ConOps. In the event of a conflict between the referenced document and this document, this document shall take precedence. The following documents contain additional requirements through reference in this document:

- *N-DEx Case Incident Report; version 1.0.4 (XML Bundle)*
- *Occupational Safety and Health Administration (OSHA) Standards, Part 1910, Subpart G, Occupational Health and Environmental Control, Subpart S, Electrical and Subpart Z, Toxic and Hazardous Substances*
- *Global Justice XML Data Dictionary, most current version*
- *Title 28, Part 23 of the Code of Federal Regulations; "Criminal Intelligence Systems Operating Policies"*
- *N-DEx Executive Concept of Operations, November 30, 2005*
- *N-DEx Program Plan, 11/21/2005*
- *N-DEx Prototype Project Plan*
- *CJISCAPP, December 8, 2003*
- *Sentinel User ConOps, October 5, 2005*
- *LEISP Program Strategy, April 26, 2005*
- *FBI Information Technology Life Cycle Management Directive, Version 3.0, 8/19/2005*
- *N-DEx Memorandum of Understanding*
- *N-DEx System Requirements Specification, Version 3.1*
- *Regional Data Exchange ConOps, 6/3/2004*
- *All related Operation and Maintenance Documents*
- *Operation and Maintenance Concepts and Requirements*
- *Section 508 of the Rehabilitation Act (29 U.S.C. 794d)*
- *CJIS SoS System Engineering Management Plan*
- *CJISD-CMP-05001-1.2, dated August 26, 2002*
- *CJIS Configuration Management Plan*
- *CJIS Quality Assurance Plan*
- *FBI Manual of Administrative Operations and Procedures (MAOP)*
- *CJIS System of Services Target Architecture*
- *Los Angeles County Sheriff's Department Incident Report Schema, XML*
- *CJIS APB Security Policies*

- *FBI, Security Division Certification and Accreditation Handbook, Version 1.1, July 31,2003*
- *UCR Automation Concept of Operations*
- *UCR Automation System Requirements Document*
- *NIEM Standards Package, most current version*
- *Federal Enterprise Architecture Framework, Version 1.1, September 1999*
- *Clinger Cohen Act of 1996*
- *Brady Handgun Violence Prevention Act (Brady Act) of 1993, Public Law 103-159*
- *Notice of Proposed Rulemaking, July 2001, Title 28, C.F.R.,§25.9 (b)*
- *FBI Security Division Information Assurance Technology Infusion Program, Technical Enterprise Security Architecture Description, Version 1.0, March 30, 2003*
- *Intelligence Reform and Terrorism Prevention Act of 2004*
- *NCIC Message Book, February 23, 2006*
- *FBI Project Management Process Manual, January 2002*
- *Hate Crime Online Data Entry and Edits, December 15, 2003*
- *System Engineering Management Plan, July 2005*
- *UCR Project Data Handling Rules Technical Report*
- *III Operational and Technical Manual, 1994*
- *N-DEx Topic Papers, CJIS APB Process, Fall 2005*

Appendix E: Issues/Topic Papers

TBD