



HAMPTON ROADS LAW ENFORCEMENT INFORMATION EXCHANGE (LInX)

"FREQUENTLY ASKED QUESTIONS"

*A Guide for Current LInX Participants, Future Participants
And the Public*

July 1, 2004



Table of Contents

1.0 Introduction	1
1.1 Scope	1
2.0 Background	2
2.1 Project Origin	2
2.2 Regional Data Sharing	2
3.0 User Questions	3
3.1 Who pays for the cost of the LInX system and what will it cost me?	3
3.2 Who determines what information is provided to the LInX system?	5
3.3 How are records deletions controlled in the LInX system?	5
3.4 What do I have to do to contribute information to the LInX system?	6
3.5 How much information do I have to divulge about my system and network?	6
3.7 Who controls access and administers the LInX system	8
4.0 Privacy Questions	8
4.1 What is the Privacy Impact Assessment and the Privacy Impact Statement	8
4.2 Can direct legal action result from a LInX query?	8
4.3 Will the LInX contain intelligence data or files?	9
4.4 Is the content of the LInX system "Secret" or classified?	9
4.5 Who has oversight of the LInX system?	10
4.6 What information will the LInX system contain?	10
4.7 Is the LInX a legal entity?	11
4.8 Is a participating agency allowed to make a secondary dissemination?	11
4.9 Who owns the data in the data warehouse?	11
4.10 How are Freedom of Information and PA requests handled?	12
5.0 Other Questions	13
5.1 Who is participating in the Hampton Roads LInX system?	13
5.2 How does LInX gain access to law enforcement information?	13
5.3 How will LInX protect investigative data?	14
5.4 What are the levels of access built into the system?	14
5.5 How will LInX comply with legal requirements such as 28CFR?	14
5.6 What data formats can be imported into the data warehouse?	14
5.7 What data base management system does the LInX system use?	15
5.8 What are the basic capabilities of the LInX system?	15
5.9 Will all capabilities be available to all users?	15



5.10	What is geo-spatial mapping?	15
5.11	How much of the data can be geo-coded and displayed on a map?	16
5.12	What are link diagrams?	16
5.13	What hardware is required for users to access LInX?	16
5.14	What is a data warehouse?	16
5.15	What does auditing mean?	17
5.16	How will the LInX system be evaluated?	17
6.0	An Example of Use	20
6.1	Are there examples of how the LInX system can or will be used by the law enforcement community?	20



1 Introduction

Over the past several years, federal, state, and local law enforcement have experimented with information sharing on an unprecedented level. The Naval Criminal Investigative Service's (NCIS) Law Enforcement Information Exchange (LInX) initiative is one of these efforts being developed to test the effectiveness of capturing and fusing the cumulative criminal justice knowledge of federal, state, and local law enforcement agencies from a region. When fully implemented, it is expected that this initiative will have enhanced the coordination of law enforcement action as well as the effectiveness of participating law enforcement agencies by identifying, neutralizing and dismantling the most significant criminal and terrorist organizations operating in the region, thereby dramatically reducing the threat of terrorist acts while significantly impacting crime in the communities. Additionally, the system will allow unprecedented information for local and regional crime solving, crime prevention and suppression as well as enhance officer safety.

Specifically, the mission of the Hampton Roads LInX system is to facilitate the timely sharing of accurate criminal justice data across the region for the purpose of more efficiently identifying criminal and terrorist organizations and activities, recognizing crime patterns, suppressing and reducing crime and protecting critical national assets, thereby enhancing public's safety.

1.1 Scope

This document provides a brief background on the LInX project, and then addresses some of the questions one may ask about becoming a member of the Hampton Roads LInX system. The intent of this document is to answer as many questions as possible about the system. It is anticipated that this document will grow over time to incorporate new information and questions as the project more fully develops.



2 Background

2.1 Project Origin

The Naval Criminal Investigative Service is the organization within the United States Navy with primary responsibility for criminal, counterintelligence (CI) and counter-terrorism (CT) investigations and operations, as well as Navy security and law enforcement policy matters. NCIS has primary responsibility for liaison on all criminal investigative and CI matters with federal, state, county and local law enforcement and intelligence agencies. The Hampton Roads LInX project is designed to address issues that arose from the attack against the USS COLE and the September 11, 2001 attack on the United States. These acts of aggression dramatically accelerated the need for change in all areas of NCIS operations, providing impetus for NCIS to act quickly and prudently to address critical, emergent mission challenges. NCIS has initiated the LInX effort to ensure effective information sharing with the state and local law enforcement agencies within selected regions of the country where critical naval assets are located.

2.2 Regional Data Sharing

An information-sharing effort in the Hampton Roads Region, the Comprehensive Regional Information Management and Exchange System (CRIMES), was in place as a joint project among seven local law enforcement agencies prior to the terrorism events of September 11, 2001. However, because of the numerous Navy interests in the region, NCIS volunteered to build, fund and implement the first phase of LInX, a dramatic enhancement to the existing information sharing capability. To adequately protect these sensitive Navy interests, NCIS understood the need for an increasing amount of information sharing technology, instant situational awareness, analytical capabilities and robust collaboration among and across multiple levels of law enforcement agencies in and around Hampton Roads.

LInX does not create new law enforcement records only new capabilities in gathering, integrating, analyzing, linking and fusing existing records already contained in participating agencies' in-house records management systems. LInX provides investigators the ability to know things not previously known and analysts the ability to detect and analyze crime trends and criminal organizations across a region instead of only within a locality.



3 User Questions

3.1 Who paid for the cost of the LInX system and what will it cost me if I choose to join?

The Hampton Roads LInX project is sponsored by the Naval Criminal Investigative Service (NCIS).

For the original member agencies NCIS has paid for:

- The cost of the LInX hardware and software;
- The cost of the LInX contractor to fully integrate the existing system with LInX;
- The cost to provide “train the trainer” training; and
- The cost of maintaining the hardware and software system for at least the first year after full system deployment.

Participating user agencies contributed:

- The limited labor necessary to interface to the LInX system;
- The limited labor necessary to train their agency users;
- Access to or extracts from agency records management systems (RMS) and available investigative files;
- Any technical updates or revisions a locality chose to make outside of the LInX system; and
- NCIS did not cover the cost of participating agency staff salaries.

The LInX project has minimized the amount time and effort required by the participating agencies to support the project.

In general, an agency’s IT representative:

- Participated in the technical working group meetings conducted once a month, or as required;
- Conferred with the contractor’s LAN engineer one or more times for “a couple of hours” each to determine how to connect the existing RMS to the LInX System; and
- Met with the contractor’s system architect two or three times for “a couple of hours” to determine what data are available, what data the agency will be contributing and how the agency will make the data available to the LInX system.



Once this information was made available, the LInX designers developed the design and the LAN engineer developed a network interface to the agencies. This information was shared with the agency so the agency could prepare for the arrival of the LInX system. This required the agency's network engineer to configure the network to accept a LInX connection.

The LInX contractor worked closely with the existing records management system vendor to get detailed record formats and interface information if this information was not readily available from the agency IT staff. The agency only needed to inform the records system vendor it has the authorization to talk with the LInX contractor.

The total anticipated time required of the agency participants is measured in hours totaling approximately three days over the period of the project.

The LInX project will maintain all software, the data warehouse, the three applications servers, the network connections and the triggers that move the RMS information to the warehouse. Front porch servers for any new agencies will be the responsibility of that agency.

Agencies who wish to join LInX in the future will be required to connect to the existing system through a data replicator and to pay for:

- The cost of the data replicator (front porch server);
- The cost for software and licensing to operate the front porch server;
- The cost for the LInX maintenance contractor to connect, transfer, index and integrate your information into the existing system; and
- Covering the cost of training users within your agency to fully understand and use the system.

In addition, agency personnel will be required to participate in the meetings as outlined in the paragraphs above.

The agency's systems administrator will add the LInX server interface to the computer domain so agency data can be moved to the front porch. The LInX contractor will arrange a time to install the front porch server in the agency. These tasks should take less than a day. The agency should provide an escort for the contractor while the contractor is in the facility. The contractor will install the server, connect to the network, test the interface back to the central database and, then test the interface to the agency's records system. This process should take two days or less. During that time the contractor will need an escort, two to four hours of time from the network support group and 4 to 6 hours of support from the IT group to test the interface with the CAD system.



3.2 Who determines what information is provided to the LInX system?

The Board of Directors determines what information will be stored in LInX. Each user agency will determine the data it wants to contribute to the LInX system within the guidelines proffered by the Board of Directors. Most CAD, RMS, and records systems contain a large amount of information that is beyond the scope of the LInX system. The LInX system does not include nor want:

- System password files;
- Personnel files;
- Personal information on officers or employees;
- Sensitive investigative information such as public corruption cases;
- Data on undercover operations;
- Data about nor internal affairs investigations;
- Intelligence data; and
- Any information that would compromise an officer's safety or any sensitive investigation.

The LInX system should contain all available information on:

- People, places, incidents, arrests, vehicles, crimes, contacts, weapons, pawned items, field interviews;
- Mug shots to identify persons during traffic stops or investigations; and
- Unstructured data such as investigative case reports and narratives, follow-up reports with available narratives and investigator case information.

3.3 How are records deletions or purges controlled in the LInX system?

The LInX system has a direct interface with most agencies' records management systems and a front porch interface to the remainder of the agencies' records management systems. The LInX system automatically detects any change in the status of the records (a deletion in this example) in an agency's RMS electronically and immediately changes (or deletes in this example) that record in the data warehouse to, again, reflect an exact copy of the RMS data. This applies to both structured and unstructured data.



3.4 What must an agency do to contribute information to the LInX system?

The majority of the work to connect and contribute to the Hampton Roads LInX system has been performed by the NCIS contractor. As described above, NCIS purchased the software and hardware. Each agency provided assistance to the contractor to connect to the LInX system by providing qualified support on a limited part-time basis.

The Hampton Roads LInX data warehouse has been installed at the NCIS office at the Washington Navy Yard in Washington, D.C. All initial participating agencies have been connected to the server directly through the agency's RMS. This is called a distributive system. Some agencies, however, have since implemented a front porch to collect and transport the agency data to the data warehouse.

New agencies that wish to participate will utilize the front porch concept. Also, multiple agencies may join through a regional network and will be connected to the LInX System as a group. A single front porch can be installed to service the entire group of agencies, depending upon the volume of data.

3.5 How much information must an agency divulge about its system and network?

LInX is interested in the following information from participating agencies' systems:

- Sufficient network knowledge to connect/interface to the user agency;
- Sufficient records management system knowledge to receive data from the agency; and
- Sufficient security policy information to ensure the security of LInX and the security of the agency's network.

LInX does not want to know:

- The entire layout of an agency's network;
- The password or identifications from any of the agency's systems;
- Access to restricted or sensitive agency data; or
- Administrative privileges on agency computer systems.

As discussed herein, LInX will develop a security accreditation policy to ensure the system meets a minimum set of security standards. The information collected to accredit the system will not be disclosed to the public. The document is for use by the federal



sponsor and the other federal participants, and as such will be secured and treated as sensitive law enforcement data.

3.6 What security standards does LInX use?

The United States Navy must accredit the LInX system according to the Department Of Defense (DOD) Information Technology Security Certification and Accreditation Process (DITSCAP). This standard will be used to set the minimum standard the LInX system must meet based on the security level of the data stored in the system. The LInX system has been declared a sensitive but unclassified system, and it will contain **no** information above the *law enforcement sensitive* level. The accreditation process is a comprehensive assessment of the entire LInX system. The accreditation addresses three major areas; integrity, availability, and confidentiality. Each of these three areas is broken down to physical, personnel, administrative, information, information systems, and communications. A System Security Authorization Agreement (SSAA) for compliance with the DITSCAP standards, accreditation and the certification is available.

All information flowing through the LInX system outside an agency's facility is encrypted. The encryption process will use triple DES 128-bit encryption. The network used by LInX is the Commonwealth of Virginia's Covanet, a virtual private network (VPN) that also transmits police data for AFIS, VCIN, LIVESCAN and TIPS to localities.

The accreditation group will talk with each agency to first ensure the DITSCAP accreditation process addresses all the agencies concerns and is compliant with the individual agencies security standards. As stated above, this process sets the minimum accreditation and security standards for the system. The standards will be modified as necessary to ensure the SSAA addresses the security concerns of the LInX user community.

After the accreditation process is complete and documented, the accreditation group headed by NCIS will perform an audit. They will visit each agency to ensure:

- The agency has at least the following policies and procedures in place:
 - Minimum size of a password (8 char.);
 - How often the passwords are changed (120 days maximum.);
 - How users are trained to log off the system when not in use; and
 - The agency performs regular security audits.
- The front porch server is secured in a controlled access area;



- There is an access control policy to prevent unauthorized access to the equipment; and
- The agency has disseminated and is in compliance with the Board of Directors Security Policy.

3.7 Who controls access and administers the LInX system?

The overall governing authority for the LInX system will be the Board of Directors. They will set system-wide policies and procedures. The Board of Directors consists of the CEO, or his or her representative, from each participating agency.

Each agency will have a system administrator and security administrator assigned to the system. The primary administrator can assign additional administrators or administer the system him or herself. Each agency will be able to add, change or delete users in the agency and reset passwords internally. The security administrator will have the ability to monitor system usage by:

- Viewing who was using the system and for what date, time and duration;
- Viewing the queries made by user ID (the system logs the query results); and
- Viewing failed attempts to access the system.



4 Privacy Questions

4.1 What is the Privacy Impact Assessment and the Privacy Impact Statement?

The Privacy Impact Assessment (PIA) is a documented assessment of the entire LInX system that includes information such as:

- The type of information/data in the system;
- System management;
- Who uses the information;
- How agencies access the information;
- What controls are in place to prevent misuse;
- The attributes of the data in the system;
- The potential effects of the system on an individual's privacy;
- Classification of the information in the system; and
- Maintenance of administrative controls.

The Privacy Impact Statement addresses the issues raised in the PIA and establishes guidance and direction to ensure that the privacy of individuals are being safeguarded.

Both the PIA and the Privacy Impact Statement are documents that are prepared and maintained as part of the accreditation process for the Hampton Roads LInX system. These documents are maintained by the sponsoring federal agency (NCIS).

4.2 Can direct legal action result directly from a LInX query? (How will it be used?)

The data content of the LInX system will not be considered for use as definitive probable cause for purposes of any direct legal action including arrests, searches, or seizures. A hit alone on the LInX system is not probable cause, but is only an indicator that data, a report, or other information exists in the records management system of an identified participating agency. A positive hit in the LInX system should be considered only one element in effective law enforcement, or building an investigative case that could lead to probable cause for arrests, searches and seizures, etc.

The data from the LInX system is not considered, and should not be used for, original documentation for probable cause from any participating agency that will result in direct legal action on the part of the querying agency.



Correct LInX system procedure, as established by the Board of Directors, requires the agency that provided access to the data to be contacted by the inquiring investigator to confirm that the data is accurate and up-to-date. In some circumstances, the hit that will be confirmed with the originating agency may be the major or only element necessary to “initiate” an investigation, obtain a search warrant, detain or make an arrest. For instance, a confirmation of investigative information existing in a participating agency’s records management system on an individual, or a hit on a vehicle or property, must be confirmed through the original documentation from the original agency and not solely by utilizing the documentation obtained from the LInX query to support any activity that would likely lead to testimony. The confirmation of the validity of the information from the originating RMS would be enough cause to initiate appropriate and reasonable action.

Records such as the Violent Gang, Terrorist Organization, Convicted Persons on Supervised Release, Convicted Sexual Offender Registry, Protection Orders, and other officer safety alerts that may be included within the LInX system do not require immediate hit confirmation. They are designed to provide law enforcement officers with adequate warnings regarding individuals who have had involvement in violent criminal activities or are known to represent potential or immediate danger to the investigative officer and/or the general public.

4.3 Will the LInX contain intelligence data or files?

The Hampton Roads LInX system will contain only law enforcement information obtained from existing police records management systems. The initial LInX system is not intended for the storage of law enforcement intelligence information.

At some time in the future, if appropriate funding is received and legal issues are met, the LInX system could provide for the storage and analysis of law enforcement intelligence information.

4.4 Is the content of the LInX system “Secret” or classified?

As stated above, the information contained in the LInX system is not classified above the sensitive law enforcement level (unclassified). All of the information contained in the system is derivative investigative information obtained from municipal, county, state and federal records systems.



4.5 Who has oversight of the LInX system?

The Hampton Roads LInX system operates under a shared management concept among the federal, county and municipal law enforcement participating agencies and users. The body charged with managing the LInX system is referred to as the Board of Directors.

The operational concept and design of the LInX system is intended to be managed and controlled by the Board of Directors which consists of the CEOs from all of the participating or contributing agencies in the region. The Board of Directors acts as an advisory and policy board assuming responsibility for the administrative and operational control of the system. The Board of Directors is responsible for access to all aspects and levels of the LInX system data warehouse by all of the authorized agencies within the region, who are participating with the approval of the Board of Directors

The Board of Directors has the responsibility for the establishments of:

- A Charter;
- A Memorandum of Understanding (MOU);
- Rules for operating the system;
- Privacy Impact Assessment and statement;
- Security plan;
- Security policy;
- Membership and level of participation;
- Potential enforcement of misuse sanctions;
- System planning, deployment and administration; and
- System enhancement and grant management along with approving the necessary hardware and software for use on the system.

The Board of Directors may delegate some of these duties, but in all cases the Board is the final arbiter in all matters involving LInX.

4.6 What information will the LInX system contain?

Information will be collected from a number of local sources in the Hampton Roads Region. It is expected that the following categories of information will be included:

- *Police Department Automated Field Reporting*—Field interview/reporting information;
- *Police Department Records Management Systems*—investigative and follow-up investigative information in structured and free text formats;



- *Criminal Records Management System*—Data related to criminal activity;
- *Gang Information*—important data on violent criminal gangs;
- *Traffic Summons Information*—data on traffic stops from participating agencies;
- *Mugshots*—information from booking—an index of available law enforcement photographs;
- *Naval Criminal Investigative Service (NCIS) investigative information* will come from electronic investigative reports located at NCIS Headquarters; and
- *Pawn Shop Transactions*—information from pawnshops in each participating locality.

In the future it is expected to add additional information to the system including:

- *Computer Aided Dispatch/911*—Dispatch information and 911 call data.
- *Jail/Parolee Information (JIMS)*—Inmate information from booking to release.

4.7 Is LInX a legal entity?

The LInX system is a federally sponsored and funded multi-jurisdictional, joint cooperative effort to put duplicative law enforcement structured and unstructured investigative and incident data into a data warehouse, and making that data warehouse available to all participating agencies for review and analysis.

As such, the LInX system is not a legal entity, as the information contained therein is derivative information from the records management systems of the participating agencies, with the ownership of that information maintained by the contributing agency.

4.8 Is a participating agency allowed to make secondary dissemination of another agency's information without approval of the owner of the data?

As delineated elsewhere herein, in the MOU, and in the Rules of Operation for the LInX system, all of the information contributed by an agency remains the property of that agency and cannot be used or disseminated without the consent of the originating party/agency. The fact that the information has been contributed to the LInX data warehouse is not implied as permission to disseminate the information without the permission of the originating agency.



4.9 Who owns the data in the data warehouse?

As delineated elsewhere herein, in the MOU, and in the Rules of Operation for the LInX system, all of the information contributed by an agency remains the property of that agency and cannot be used or disseminated without the consent of the originating party/agency.

4.10 How are Freedom of Information or Privacy Act requests to be handled?

All Federal or State FOIA, Privacy Act or public disclosure requests for the disclosure of information or records contained in the LInX System will be made to the originating agency that maintains ownership of that information or records.



5 Other Frequently Asked Questions

5.1 Who is participating in the LInX system (which federal, state, county or municipal agencies)?

In the Hampton Roads LInX system the following agencies are the current participants:

Local law enforcement agencies:

The cities of:

Chesapeake
Hampton
Newport News
Norfolk
Poquoson
Portsmouth
Smithfield
Suffolk
Virginia Beach
Williamsburg

The counties of:

James City
York

The federal agency:

Naval Criminal Investigative Service

5.2 How does LInX gain access to state, county and municipal law enforcement information?

LInX takes advantage of existing networks and technological efforts in the Hampton Roads region by enhancing the existing information and creating new information sharing capabilities while fostering necessary agreements among all of the participating agencies. For cities without organized information sharing efforts, LInX provides the necessary help to put in place the necessary information sharing structure.

The technology used by the LInX system relies on encrypted virtual private network access between the agencies and the data warehouse.



5.3 How will LInX protect federal, state, county and municipal investigative data so as to not jeopardize ongoing investigations, confidential information, and other sensitive data?

LInX is using the most advanced technology available to put in place state-of-the-art information security tools to control access to sensitive information, to include robust authentication and role-based security access levels. Users can only access information to which they have been authorized.

5.4 What are the levels of access built into the LInX system?

There are four levels of access built into the system:

Tactical User

This level of access is provided to line or patrol officers, which will allow them to use the system for quick look-up for all names, addresses, vehicles and incidents in the LInX system. All users will have this access.

Investigative/Analytical User

This level of access is provided to allow designated criminal investigators and analysts access to see all structured and unstructured or “free text” source documents, conduct analysis on those documents and provide link analysis for the information contained therein.

Administrative User

This level of access is provided for system administrators. There is at least one in each participating agency.

Security Administrative User

This level of access is provided for administrative, security and audit purposes. This is at least one in each participating agency.

5.5 How will LInX comply with legal requirements such as 28 CFR?

LInX is not an intelligence network therefore it does not come under the purview of 28 CFR Part 23. However, NCIS and legal counsel have conducted a study of the impact the LInX effort will have on privacy and confidentiality. If, in the future, 28 CFR Part 23 becomes applicable to the system, every effort will be made to comply with all legal and



regulatory requirements. It will also make sure that state privacy and confidentiality requirements are supported by this effort. Some of the issues that have been addressed include—secure storage of information, inquiry/search/audit capability, controlled dissemination, public disclosure and the review and purge process.

5.6 What data formats can be imported into the LInX data warehouse?

The LInX System can accommodate most any and every data format. It has collected and successfully integrated structured data, such as the data in many law enforcement records management systems—citations, incident reports, pointer systems, etc. It can also integrate many unstructured forms of data, such as those created during investigations—free text, rich text format (rtf), Microsoft Word, and WordPerfect documents. LInX is using open-architecture and commercially available technology, so it can take advantage of any and all tools necessary to get the information into the data warehouse and have it available to the investigators within the community.

5.7 What database management system does the LInX system use?

The LInX system is built on an Oracle relational database management system (RDBMS). NCIS has the appropriate licenses for Oracle and it is the leading commercial RDBMS on the market.

5.8 What are the basic capabilities of the LInX system?

For the first phase of LInX, the basic capabilities that are delivered with the system include:

- Simple queries;
- Structured data search (person, location, incident, vehicle, weapon, pawn information);
- Free text (unstructured data or narratives, etc.) search;
- Link analysis; and
- Officer safety alerts/comment fields.

Additional capabilities such as geo-spatial mapping will be added based upon unique needs of a particular locality as well as across the board to all agencies, as the project matures and funding is made available.

5.9 Will all capabilities be available to all users?



No. Patrol officers and other tactical level users will have access only to simple query and structured data searches which will return information on searched names, addresses, vehicles, incidents and identifying numbers such as SSN, FBI, SID, etc. Investigators and analysts will have access to all of the LInX capabilities.

5.10 What is geo-spatial mapping?

Geo-spatial mapping is a technology used to display data on a regional or local map grid. The data that is entered into the data warehouse is geo-coded with the map coordinates allowing addresses, persons and incidents to be mapped directly to regions, cities, or neighborhoods.

5.11 How much of the integrated data can be geo-coded and displayed on a map?

All data to be integrated into the data warehouse can be geo-coded.

5.12 What are link diagrams?

Link diagrams are visual representations of relationships between people, addresses, vehicles, incidents, documents, etc., from the collected information in the data warehouse. The Hampton Roads LInX system utilizes the Visualinks™ link analysis and search tool that will assist investigators by uncovering, interpreting, linking, and displaying complex information in easily understood chart format.

5.13 What hardware is required for users to access the LInX data warehouse?

The LInX data warehouse only requires a standard PC and a web browser, and the appropriate access level assigned by the system administrator. It is envisioned that in a future phase, patrol officers and investigators will be able to access the LInX data warehouse via hand-held devices and other wireless technologies.

5.14 What is a data warehouse?

The LInX data warehouse is a centralized computer designed and formatted to assist with investigative, strategic, and management decisions. It will contain federal, state, county and local agency data. The LInX warehouse will consist of the following components:

- *Data Dictionary* – Describes the data elements, formats and textual description of the purpose and about the structure of the data in the system. The Data Definition



- Language will be used to describe tables, columns, indexes, relationships and constraints;
- *Data Extraction and Transformation Tools* – Tools that allow the warehouse to extract data from law enforcement records management systems, transport that data to the warehouse and then normalize it for use by all agencies; and
 - *Analysis and End User Tools* – Tools used in the LInX data warehouse include various online analytical processing tools described below. This component makes the system functionally viable as an analytical system.

Users can produce topic chronologies, analytical summaries, time lines, charts, and graphs. Linkages and chronologies are based on information supplied from multiple agencies, thereby painting a more complete picture of the activity of individual criminals as well as the impact of criminal organizations in the region. The structure of the warehouse will provide relational, multi-dimensional, and hybrid forms of on-line analytical processing. The processes implemented for maintaining the database (e.g., data extraction, transformation and loading) will simplify the importation of data from the contributing agencies.

5.15 What does auditing mean?

The LInX data warehouse includes the capability to audit the entire system and its users. The system logs all user actions to include who has used the system, time and date of user queries, actual queries executed, alerts set, notifications received and failed login attempts. The logs are capable of being archived, so if the server hard drive space needs to be freed, the logs may be moved to a tape or other non-volatile storage medium. A permanent tape backup will be maintained in compliance with public disclosure and FOIA requirements.

5.16 How will the LInX system be evaluated?

Criteria to evaluate the system is required to ensure that the public is receiving the most effective tools available for use by law enforcement and that the system being deployed is meeting the needs of the community.

A critical evaluation will help assess the operational utility of the initiative based on criteria identified as the most significant characteristics of successful information sharing.

These criteria take into account seven major areas:



1. *Strategy* — The project must have the ability to address specific criminal or terrorism issues and other tactical and strategic law enforcement concerns as identified by the Board of Directors;
2. *Governance* — The project must establish a governance infrastructure to support policy and operational decisions for the long-term viability of the project;
3. *Data* — The depth and breadth of data must be sufficient and fully integrate structured and unstructured investigative data with other requisite internal and external data;
4. *Capabilities* — It must have the operational and technical abilities necessary to support effective law enforcement action;
5. *Technology* — The technology must be built upon open standards and leverage and enhance existing systems;
6. *Support* — The project development and delivery must include a robust user training and technical support capacity; and
7. *Evaluation methodology* — The project must have identified evaluation criteria to evaluate the effectiveness of the system to law enforcement operations.

These criteria will help determine the overall impact of the project and will gauge the probability for long-term operational success. These are further described as:

Strategy The project must identify specific criminal or terrorism related law enforcement outcomes that are to be achieved through information sharing. The outcomes would be based on specific federal, state, county or municipal terrorist or crime threat assessments.

Governance The project must formally address governance issues, such as federal, state, county and municipal information management protocols and processes to aid in decision making regarding data to be shared, data ownership, data/system access, security, privacy impact, agency participation, and compliance with legal and regulatory requirements.

Data The appropriate depth and breadth of data including structured police reports, free-text investigative reports, suspicious activity reports, CAD data, and other law enforcement related information pertinent to achieving a successful outcome to tactical, investigative and analytical queries. The type of data to be included must be driven by the anticipated benefits and achievement of the strategy. It must go beyond structured records management data (commonly shared now) to include all available investigative case files.



Technology The technology utilized must be built upon open architecture and have the capability to expand and enhance the system according to future needs. Additionally, the technology utilized should enhance existing systems, not force the addition or creation of new records systems. The technology must provide easy and direct use by patrol and investigative personnel otherwise maximum usage by law enforcement personnel will not be achieved.

Capabilities Information sharing initiatives should have the following capabilities:

- Automates analytic processes normally accomplished by people;
- Provides single query across the entire range and scope of data;
- Simultaneously searches the full set of unstructured and structured documents;
- Automatically generates link diagrams based on an automated analytical process;
- Plots search results on a visual display, with direct access links back to the related data;
- Provides immediate notification about the law enforcement status of any subject of interest;
- Supports predictive analysis to discover/track crime trends and support strategic initiatives;
- Integrates and/or leverages existing federal, state, county, and local information sharing efforts;
- Provides robust user authentication, auditing, and security;
- Includes multi-jurisdictional, layered access to data; and
- Includes data purging to comply with federal, state, county, and local laws, rules, and protocols regulating system privacy, security, and integrity.

Support To be effective the project must provide operationally focused user training and technical support. The training must go beyond teaching the use of specific operational “buttons”, but should also include how to use the information-sharing project to directly support tactical, investigative and strategic law enforcement activities.

Evaluation There must be documented evaluation criteria, derived from the anticipated law enforcement outcomes that the project will use to gauge success. These criteria should include, at a minimum, the ability to demonstrate that the project:



-
- Provides new information to all levels of the law enforcement community that they otherwise would not have had;
 - Provides a multi-agency perspective of criminal activity, involving all jurisdictional levels of law enforcement;
 - Enables cross-jurisdictional analysis of all available investigative information;
 - Introduces and integrates external data not generally available to law enforcement;
 - Provides demonstrable, multi-jurisdictional investigative impact across all jurisdictional boundaries;
 - Provides the ability to link terrorism subject movement, associations and law enforcement contacts with intelligence to identify potential threat sources, fund raising activities, and criminal activity linked to terrorism; and
 - Quickly develop crime trends across regions as opposed to addressing isolated incidents within specific jurisdictions without the knowledge of criminal associations or an interrelationship.



6 An Example of Use

6.1 Are there any examples of how the LInX system can be used by the law enforcement community?

The following scenario has been provided to illustrate how LInX can be used and positively affects users of the system (it is based on actual facts). This scenario is based on realistic crime trends related to petty burglaries, along with a potential solution and the impact on regional crime.

Background:

- Local police departments are experiencing the reporting of petty residential and business burglaries.
- No pattern is noted due to the nature of the break-ins and the low level of related thefts.
- Thefts generally involve jewelry, cash, checks, and as reported “other miscellaneous documents.”
- Negligible or no physical or forensic evidence is noted in any of the cases.
- Burglaries occur approximately two to three per week in each community.
- After exhausting any scant leads, the local police departments place the cases in a “pending-but-inactive” status due to the low priority of the offenses. Experience has shown the nature of these crimes is such that these types of burglaries tend to be juvenile related.

Issues:

- Based on normal investigative techniques these cases probably would not be solved due to the low level of the activity, no set pattern, lack of evidence and lack of priority based on other investigative responsibilities and limited resources.
- Generally the only way these offenses are solved is through a “lucky break” (something administrators hope for so they aren’t required to exhaust limited resources on low-level crimes), with the arrest of an individual who has knowledge of the cases, and who is willing to provide information in return for favorable consideration in his or her own criminal case.
- Most cases of this nature will not be solved through the initiative of investigators who are also responsible for crime investigations involving rape, robbery, homicide, etc.



LInX System:

Through the use of the LInX system, the following would be available to investigators about an individual locality as well as on a regional basis:

- All of the related regional burglary information is included in the data warehouse along with the other federal, state and local investigative information from each localities' RMSs, CAD systems, suspicious activity reports, etc.;
- Information from all jurisdictions would be linked through normal business processes integrated by the system;
- Crime analyst usage of the system, not valuable investigator time, would be used to analyze crime patterns and crime problems within the community; and
- Once the number of these types of burglaries reaches a preset trigger, the analyst(s) will conduct a basic query of the system based on victim's name, addresses, property taken, etc. as a normal course of business for the department.

Impact:

With this system in place realistic solutions could be developed as follows:

Basic steps to success:

- An analyst or investigator is assigned to make a basic query of several of the burglaries from within their jurisdiction as a course of business;
- The analyst/investigator enters the burglary addresses into the LInX and develops a geo-spatial map of the occurrences;
- The analyst/investigator then requests inclusion of all of the burglaries from the region, for the past period that matches the Modus Operandi (M.O.) of the ones in his or her community;
- The query reveals approximately a dozen similar burglaries within the analyst/investigator's jurisdiction that are assigned to different investigators in the department, as well as several dozen more similarly assigned to multiple investigators within other jurisdictions;
- The system also reveals for each jurisdiction the pattern of activity is similar; and
- The analyst/investigator then checks the addresses in each of the reports against all other available information in the system and finds out the following links based on the resultant analytical product:
 - In a number of the instances an available field interview card or suspicious activity report notes the same three cars in the communities where most of the burglaries occurred;
 - In two instances the officers got the names of the drivers and passengers the day before any of the burglaries occurred;
 - In all instances the occupants were adult males of foreign affiliation; and

-
- Victim names were associated with low level crimes such as:
 - Insufficient funds or account closed check cashing;
 - Multiple automobile accidents involving minor injuries in alternate jurisdictions;
 - Credit card fraud cases;
 - Pawn reports of high volume sales in areas outside of the victims residency area;
 - The same names (victims) coming up in different jurisdictions associated with police contacts, (non-criminal in nature), such as speeding, accidents, requests for service calls, etc.; and
 - The Social Security numbers for the victims were associated with names different than the victims, generally foreign in nature.

This routine analysis of the LInX system showing the above associations would have been conducted in a few minutes with the results being made available to the investigator or analyst within seconds.

Possible conclusion based upon LInX usage:

- The burglaries are being conducted by an organized group who has knowledge of the level of criminal activity most law enforcement agencies will tolerate before making a major push to address the problem as a result of public opinion or internal triggers.

This organized group could be associated with one of the following:

- A local gang;
- A local (non-gang related) organized criminal enterprise;
- A national or international organized criminal enterprise;
- A terrorist organization conducting illegal fund raising;
- An independent criminal enterprise establishing itself within the community; or
- A group of juveniles as originally suspected.

In this example it appears the purpose behind the “petty” burglaries could very well be identity theft for the purpose of advancing other criminal activity.

Based upon the analysis conducted, a multi-jurisdiction investigation or task force can now be initiated to address this crime problem. Through commonalities of the concepts associated with the crimes, associated addresses, vehicles, telephone numbers, personal associates, and offenses this criminal operation can be completely disrupted in a very short period of time.



In this scenario, LInX will give the law enforcement community the ability to “connect the dots” of a possible major organized crime group, or a possible terrorist fund raising operation through the investigation of seemingly petty offenses. Without the ability afforded to the law enforcement community by LInX, these offenses would probably have gone uninvestigated until such time as the problem would have gone on far too long or have been far to large to be effectively addressed.