North Carolina
Law Enforcement Information Exchange
(NC LInX)

Frequently Asked Questions

December 2007

Table of Contents

1 Introduction

The Naval Criminal Investigative Service's (NCIS) Law Enforcement Information Exchange (LInX) Initiative has been established as the premier information sharing effort for law enforcement agencies in six different parts of the country. This effort, developed by NCIS, has clearly demonstrated through the myriad of stunning successes the effectiveness of capturing the cumulative knowledge of federal, state, county and municipal law enforcement agencies in one location, and making that information available to the law enforcement community.

LInX has been fully implemented in Washington State / Portland, OR; the Hampton Roads region of Virginia; the Corpus Christi region of Texas; Jacksonville, FL / Kings Bay and coastal GA region; the state of Hawaii; the National Capitol Region (Northern Virginia/District of Columbia/Southern Maryland); the state of New Mexico/El Paso region of Texas; Southern California (SoCal under development); and the Eastern North Carolina region (under development). This initiative has significantly enhanced the coordination and the effectiveness of all of the participating law enforcement agencies. There are currently an excess of 400 federal, state, county and municipal agencies using the seven fully operational LInX Systems.

1.1 Vision

This document will provide a brief background on the NCIS LInX Program then address some of the frequently asked questions from the North Carolina agencies about the LInX Program. This document intends to answer as many questions as possible about the first phased development NC LInX Program, while continuing to grow over time to incorporate new information and questions as the program is developed.

The overall vision of the NCIS LInX Program in the Eastern North Carolina Region is to provide added security for the U.S. Navy equities and other DoD assets, as well as address the overall Maritime Domain Awareness strategy for DoD.

The initial phased deployment will bring together 21 police and sheriff's departments with the DoD investigative organizations and the DOJ investigative entities within the Eastern District of North Carolina. The overall goal is to tie together all of the existing desperate records management systems and existing information sharing programs within the designated region. This would result in the integration of all of the agencies within the region into a common data warehouse making all of the legally sharable information available to all participating agencies.

The scope of the NCIS - NC LInX effort will tie together all of the participating agencies within the North Carolina region regardless of the records management system utilized by those agencies. The Program will also seek to maximize and improve on the existing information sharing programs being utilized in the region.

2 Background

2.1 Project Origin

The Naval Criminal Investigative Service (NCIS) is the U.S. Navy's law enforcement organization with primary responsibility for criminal, counterintelligence, and counterterrorism investigations and operations, as well as force protection, the security of Navy/DoD assets and the development of law enforcement policy matters. NCIS has primary responsibility for liaison on all Navy investigative matters with federal, state, county and municipal law enforcement and intelligence agencies. The NCIS LInX Program was established to address issues that grew out of the attack against USS COLE and the September 11th 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 initiated the LInX effort to ensure effective information sharing with federal, state and local law enforcement agencies within selected regions of the country where critical DoD and naval assets are located.

Because of the numerous Navy interests in the current LInX regions, NCIS took a key leadership role in those communities and funded the implementation of the LInX projects. The requirements to maintain effective intelligence and operational capacities demand ever-increasing amounts of information sharing technology, instant situational awareness, analytical capabilities and robust collaboration among and across all jurisdictional levels of law enforcement agencies in those areas of strategic importance to NCIS and the U.S. Navy.

2.2 Project Scope

The NCIS mission to protect those DoD assets in the Region while supporting the Maritime Domain Awareness (MDA) strategy, has created the vision for the LInX Program to act as the overall integrator and interface between the municipal, county, state and federal agencies within the region as well as the state-wide Fusion Centers being developed. The LInX Program will aggregate and integrate all of the legally sharable regional law enforcement investigative data into one data warehouse environment and make that composite data available to the officers, investigators and analysts in all of the participating agencies. The analysts and investigators within the regional Fusion Center will also have access to the information thus enhancing their overall capability to fully integrate all of the local law enforcement information into their comprehensive intelligence programs and allow them to better connect the dots.

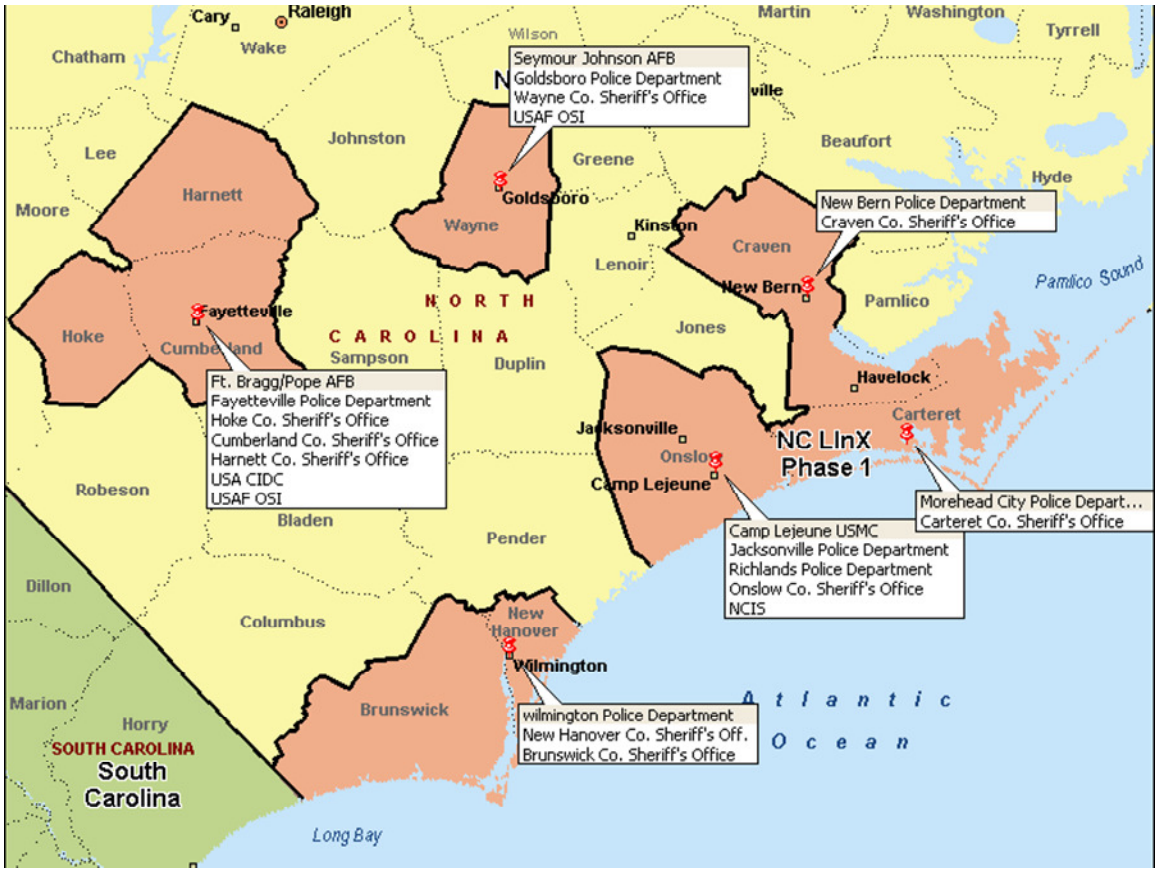
The overall impact of the LInX Program in the North Carolina region will be seen in more effective high impact terrorism and criminal enterprise investigations, and an improved ability to better address the increasing threat from all levels of cross jurisdictional violent crime.

The initial participating North Carolina municipal, county, state and federal agencies include:

1. Fayetteville Police Department
2. Goldsboro Police Department

3. Havelock Police Department
4. Jacksonville Police Department
5. Morehead City Police Department
6. New Bern Police Department
7. Richlands Police Department
8. Wilmington Police Department
9. Brunswick County Sheriff's Office
10. Carteret County Sheriff's Office
11. Craven County Sheriff's Office
12. Cumberland County Sheriff's Office
13. Harnett County Sheriff's Office
14. Hoke County Sheriff's Office
15. New Hanover Sheriff's Office
16. Onslow County Sheriff's Office
17. Wayne County Sheriff's Office
18. North Carolina State Bureau of Investigations
19. Naval Criminal Investigative Service
20. USA Criminal Investigative Command
21. USAF Office of Special Investigations

The region covered by the initial phase of the NC LInX deployment includes the following area of coverage within the Eastern District:



3 How is LInX Different?

What is the difference in all of the ongoing information sharing efforts?

3.1 CJIS N-DEx Project:

- N-DEx is proposed as a national level means to integrate *all* law enforcement information nationally.
- Proposes records management system level interconnectivity with all 18,000 state and local law enforcement agencies, or existing information sharing regional systems or networks that combine agencies.
- State and local agencies must commit resources and fund their own connectivity to the system if they wish to participate.
- Query results are limited by the types of structured incident data provided.
- A "pointer" system is the proposed level of results returned to the average state or local agency user.
- Still underdevelopment with years before full national level deployment due to the massive scope and complexity of the effort.

3.2 OneDOJ R-DEx Project:

- R-DEx is the DOJ Law Enforcement Information Sharing Program (LEISP) single source for sharing data from all of the DOJ investigative entities through a single connection to a federal data warehouse.
- Fully deployed of all available DOJ investigative information to state and locals is currently only through one location – Seattle LInX; while currently partially deployed in Jacksonville LInX (only limited FBI data available at this locations), DOJ has committed to full connectivity to all NCIS LInX Programs providing full R-DEx connectivity and access to all R-DEx information.
- Currently provides general access to limited DOJ investigative information.
- The "OneDOJ" primary focus of the R-DEx project is on solving the internal DOJ agency records sharing issues, not on promoting tangible results through comprehensive state and local sharing.

3.3 Fusion Centers:

- Effectively fuses people and agencies in a brick and mortar environment, while intelligence data is made available through agency specific terminals.
- Analysts generally have access to participating agency investigative and intelligence data through independent desperate systems requiring manual data manipulation to try to connect the dots.
- Manpower intensive program, especially for agencies with limited resources.
- Developed through grants provided by DHS with minimal standards or guidance on capabilities, governance or requirements for success.

3.4 NCIS LInX Program:

- LInX is a Government owned non-proprietary program utilizing technology solutions that are commercial off the shelf applications integrated together to provide the best operational impact for the end users.
    - The U.S. Government owns all rights and aspects of the LInX system with no vendor having any proprietary or intellectual property rights.
    - Any vendor under contract to the Government could build or leverage the LInX system, as long as they maintain the established LInX standards.
- LInX is an integrator for all levels of federal, state, county and municipal investigative data and information across jurisdictions regardless of the data source, information system or network being used.
    - It integrates all legally sharable structured and unstructured data to provide maximum operational impact for the end users.
    - Develops a composite record of all relevant data from a single query.
    - Provides for instant analysis linking associates many times removed.
- Enables all levels of existing state and local systems to achieve tangible results and interact with minimal impact on the local systems and network environments.
- Utilizes standards for each LInX site developed to ensure maximum participation and outcomes.
- Promotes and develops full governance infrastructure to ensure all levels of participation;
    - Overcomes political issues and concerns about sharing data by establishing a multi-jurisdictional partnership, establishing a structured organization and processes, with rules, policies, legal reviews, sanctions and a means for dispute resolution.
- The LInX System was designed with security as a priority requirement from the start. Each LInX system must meet and pass Federal Certification and Accreditation security standards.
- LInX was designed and is evaluated by operational users not technical developers.
- LInX has a significant track record for success in the seven fully operational locations currently in use.
    - LInX is the only acceptable environment where DHS, DOJ, DoD, state, county and municipal investigative records are shared in a fully collaborative manner.

3.5 Commercial Solutions:

- Proprietary information sharing solutions are available to the law enforcement community for purchase from private vendors.
- These solutions vary in the extreme in their capabilities and are generally implemented without adhering to any acceptable government standards.
- Most commercial solutions are highly proprietary making them expensive to deploy, effect changes, provide for maintenance, or add agencies once they are deployed.

3.6 Summary:

The non-commercial information sharing efforts are being developed and rolled out by different U.S. Government Departments with similar long range goals, but with different budgets and minimal or no interdepartmental coordination or collaboration.

- Utilizing the LInX Program as the backbone/foundation for the North Carolina law enforcement regional information sharing as well as supporting the current and future Fusion Centers, would provide a base for more effectively integrating all of the law enforcement records and information together in a regional manner.
- LInX will provide R-DEx, N-DEx, and other Federal law enforcement information sharing efforts with a standardized source of data that will allow them to more effectively connect the dots.

4 User Information:

4.1 Who determines what information is provided to the LInX System?

The Governance Board determines what information will be stored in LInX. Each user agency will provide all legally sharable data to the LInX System within the guidelines of the Governance Board. Most CAD, RMS, and records systems contain a large amount of information that may be beyond the scope of the LInX System. The LInX System does not want:

- System password or admin files;
- Officer/personnel profiles;
- Personal information on officers or employees;
- Classified investigations;
- Data on undercover operations;
- Data on internal affairs investigations;
- Clearly identified intelligence data;
- Any information that would compromise officer safety or any sensitive investigation;
- Medical information or any restricted records.

The LInX System should contain all of the legally sharable information on:

- Incidents – arrests, crimes, contacts, weapons, field interviews, citations, etc.;
- Mug shots and booking records;
- All investigative case reports, follow-up reports with available free text narratives.

4.2 How are records deletions or purges controlled in the LInX System?

With the LInX front porch interfaced to an agency's RMS, LInX picks up the record deletion information from the RMS electronically during the update process. LInX will delete the record automatically from the data warehouse. The LInX contractor will assist each agency with filtering the RMS data into the warehouse.

If the LInX System receives an electronic extract (i.e. data directly pushed from the agency RMS, CD ROM, etc.), and the record deletion is in the electronic file, LInX will delete the record automatically from the data warehouse during the update using the extract provided.

If LInX receives written reports or unstructured (free text) data and a report is deleted, the user agency must notify the LInX administrator of the deletion. The LInX administrator will then delete the record and confirm the deletion back to the requesting agency.

4.3 What must an agency do to contribute information to LInX?

The majority of the work to connect and contribute to LInX is being performed by the developmental contractors and vendors.

The LInX data warehouse must be installed in a secure location that can meet acceptable security accreditation standards. Participating agencies will be provided full access to the front porch to collect and transport the agency data to the data warehouse. Some agencies that participate in a larger regional network or commercial sharing solution (such as

Coplink), will be connected to the LInX System as a group via an interface or front porch with that solution. A single front porch can be installed to service an entire group of regionally networked agencies regardless of the source of the information.

4.4 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;
- Sufficient security policy information to ensure the security of LInX and the security of the agency's network;
- Current data schemas to permit accurate data mapping.

LInX does not want to know:

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

As discussed herein, LInX has developed strict security standards and policies as part of an established certification and accreditation process, to ensure the system meets acceptable federal security standards. The information collected to accredit the system will not be disclosed to the public. The subsequent documentation is for use by only those participants as necessary to meet the security requirements, and as such will be secured and treated as sensitive law enforcement data.

4.5 What security standards does LInX use?

Currently the U.S. Navy accredits the LInX System according to the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). This process has been 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, unless otherwise established by the Governance Board in conjunction with NCIS. The federal certification and accreditation process is a comprehensive assessment of the cyber and physical security for 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 will be prepared, maintained by the NCIS Program Management Office and made available for the site Governance.

All information flowing through the LInX System outside a participating agency's facility is encrypted. The encryption process between the user and the data warehouse uses "at least" 256 bit encryption. The encryption process within the enclave of the data warehouse security infrastructure uses 1024 bit encryption.

As a LInX user agency and participant, the accreditation group will talk with each agency to first ensure the DITSCAP accreditation process addresses all the agencies concerns and policies, as well as being 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 all of the security concerns of the LInX user community.

The accreditation process includes required audits of each system and ensures:

- 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 (90 days Max.);
    - Users are trained to log off the system when not in use;
    - The agency performs regular security audits.
- The front porch server (if one is required to be located within the agency network or facility) is secured in a controlled access area.
- There is a physical access control policy to prevent unauthorized access to all LInX equipment.
- The agency is in full compliance with the accepted Security Policies.

4.6 Who controls access and administers the LInX System?

The overall governing authority for LInX is the Governance Board. This Board sets system wide policies and procedures for the LInX Region.

Each agency will have a system administrator and security administrator assigned to support the system. The system administrator can assign additional administrators or administer the system personally. Each agency is able to add, change or delete users for that agency and reset passwords internally.

The security administrator has the ability to monitor system usage by:

- Viewing who was on the system for what period of time;
- Viewing the queries made by user ID (the system logs the query results);
- Viewing failed attempts to access the system.

Unless otherwise approved by the LInX Governance Board, the System Administrator and the Security Administrator within a single agency are not the same person. These positions should/will not have the ability to cross perform functions to ensure the maximum level of security and control on system information by all participating agency personnel.

All activities in LInX by all levels of users is subject to complete audit on at least a semi-annual basis or as directed by the Board or the NCIS PMO. In matters involving individual agencies, the head of any participating agency can request an independent audit of all information contributed by that agency from his Security Administrator.

Oversight policies are put in place to address system misuse with appropriate and enforceable sanctions.

4.7 How will the Fusion Centers interface with LInX?

The LInX data warehouse will be located in a secure federal facility to provide for maximum security. Upon agreement and approval of the Governance Board, the North Carolina Fusion Center analysts will have direct access to all of the data contained within the system. Most Fusion Centers utilize distributive search tools that will have the capacity to query the LInX system and return results to the intelligence analysts in the Centers without compromising the security of the LInX System. The analysts will have the ability to utilize the search results in ongoing analytical products used to address terrorist threats within the greater North Carolina area while remaining in full compliance with the established user agreements and rules of operation.

As a result of the LInX system being incorporated into the Fusion Centers the analysts and investigators will have unprecedented access to all of the legally sharable law enforcement information within Eastern North Carolina, regardless of the source of that data.

4.8 Will intelligence data be made available to the LInX users?

The access that the Fusion Center analysts will have to the LInX System will be a one-way query capability only, where the Fusion Centers may conduct a query of the LInX system, but the LInX users will not have knowledge of or access to any of the Fusion Center intelligence systems through the LInX system. No aspect of the Fusion Center will be accessible by any LInX user through LInX. All activity of either level of user will be fully audited in compliance with all system privacy and security requirements.

5 Privacy Questions

5.1 What are the Privacy Impact Assessment and Privacy Impact Statement?

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

- The type of information/data in the system;
- System management;
- Who will use the information;
- How will 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;
- Maintenance of administrative controls.

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

Both the PIA and the Privacy Impact Statement are documents that are prepared and maintained as part of the accreditation process for each LInX System. These documents are maintained by the sponsoring Federal Agency. A PIA must be prepared for all federal information sharing efforts.

5.2 Can any level of legal action result directly from a LInX query? (How will the system be used?)

The data content of LInX will not be considered available for use as definitive probable cause for purposes of arrests, searches, or seizures or other legal action that will require any court testimony.

A hit alone on the LInX System is not probable cause, but is an indicator only 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 for building an investigative case that could lead to probable cause for arrests, searches and seizures, etc.

By written and adopted LInX Policy, 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 procedure requires the agency which provided access to the data be contacted by the inquiring investigator to confirm that the data is accurate and up-to-date. In some circumstances, the hit which 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, event or property, must have a confirmation made from the original documentation

from the original agency and not solely rely on or utilize the documentation obtained directly 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 could be enough cause to initiate appropriate and reasonable action.

Records relating to Violent Gangs, Terrorist Organizations, 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 and are designed to provide law enforcement officers with adequate warning regarding individuals who have had involvement in violent criminal activities or are known to represent potential or immediate danger to the officer and/or the general public.

5.3 Will the LInX contain intelligence data or files?

The LInX System will contain only law enforcement investigative information obtained from existing police records management systems which will include jail and booking records. The LInX System is not intended for, and will not be used for the storage or commingling of law enforcement intelligence information.

The LInX System could provide the capacity for interfacing with a separate system used for the storage and analysis of law enforcement intelligence information, but that interface will consist of a query only capacity. No intelligence will be move to, accessed by or stored in the LInX System.

5.4 Is the content of the LInX System "Secret" or classified?

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

LInX has the capacity to interface with classified systems, but only to allow those systems to make one-way secure queries of the LInX System. Classified systems would not be queried from the LInX System and no classified data would be transferred or stored in the LInX data warehouse.

5.5 Who has oversight of the LInX System?

The LInX System operates under a shared management concept between the participating federal, state, county and municipal law enforcement agencies and users. The body charged with oversight of the North Carolina LInX System is referred to as the Governance Board.

The operational concept and design of LInX is intended to be managed and controlled by the Board which consists of the heads from the participating or contributing agencies. The Governance Board acts as an advisory and policy board assuming responsibility for the administrative control of the system. The Board assumes responsibility for all aspects of the LInX Program by all of the authorized agencies within the region, who are participating.

The Board will establish the:

- Charter;
- Memorandum of Understanding (MOU);
- Rules for operating the system;
- Privacy Impact Assessment and Privacy Statement;
- Security Plan;
- Security Policy;
- Defined membership and level of participation standards;
- Potential enforcement of misuse sanctions;
- System planning, deployment, expansion and administration;
- System enhancement and grant management along with approving the necessary hardware and software for use on the system.

Some of these duties may be delegated to a Governance or other supporting committee, but in all cases the Governance Board is the final arbiter in all matters involving any operational policies that impact the LInX Program in the North Carolina area.

5.6 What information will the LInX System contain?

Information will be collected from a number of federal, state, county and municipal sources and will include all information that can be legally maintained within a law enforcement agencies records management system, to include at least the following categories of information:

- Police Department Automated Field Reporting—Field interview/reporting and structured incident level information;
- Police Department Records Management Systems—investigative and follow-up investigative information in structured and free text formats;
- Computer Aided Dispatch/911—Dispatch information and 911 call data;
- Criminal Records Management System—Data related to criminal activity;
- Jail/Parolee Information (JMS)—Inmate information from booking to release;
- Gang Information—important data on violent criminal gangs;
- Law Enforcement Photo Information—index of available law enforcement photographs;
- Naval Criminal Investigative Service (NCIS), U.S.A.F. Office of Special Investigations (OSI), and the U.S. Army Criminal Investigative Command (CID) investigative information comes from electronic investigative reports located at the agency Headquarters;
- DOJ agency investigative information will come from electronic investigative reports contributed from systems located at the agency's headquarters. The data will be contributed either through the DOJ R-DEx data sharing system or placed directly into the LInX System. The DOJ data includes the FBI, DEA, ATF, USMS and Bureau of Prisons for the North Carolina region.

- ICE will contribute investigative and other immigration data through their internal systems as an interface through ICEPIC with the LInX Program.

5.7 Is LInX a legal entity?

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

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, where the ownership of that information is strictly maintained and fully controlled by the contributing agency. The LInX data warehouse is not a system of records.

5.8 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 Memorandum of Understanding (MOU) and in the Rules of Operation for LInX, all of the information contributed by an agency remains the property of that agency and can not be used or disseminated without the consent of the originating party/agency.

The fact that the information has been exposed through the LInX data warehouse is ***NOT*** implied as permission to disseminate or use the information without the permission of the originating agency.

5.9 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 sole property of that agency and can not be used or disseminated without the consent of the originating party/agency. As such, the data warehouse is not a new system of records.

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

All Federal or State FOI, Privacy Act or public disclosure requests for the disclosure of information contained in LInX will be made to the originating agency who maintains ownership of those records. The LInX Governance Board will adopt a dissemination and disclosure policy.

All public disclosures of any information contained within any LInX System may only be disclosed in full compliance with all of the laws, ordinances or accepted regional policies.

6 Other Frequently Asked Questions

6.1 Who is participating in the NC LInX Program, (which federal, state, county or municipal agencies)?

The initial phase of the North Carolina LInX Program will consist of the following initial contributing agencies:

1. Fayetteville Police Department
2. Goldsboro Police Department
3. Havelock Police Department
4. Jacksonville Police Department
5. Morehead City Police Department
6. New Bern Police Department
7. Richlands Police Department
8. Wilmington Police Department
9. Brunswick County Sheriff's Office
10. Carteret County Sheriff's Office
11. Craven County Sheriff's Office
12. Cumberland County Sheriff's Office
13. Harnett County Sheriff's Office
14. Hoke County Sheriff's Office
15. New Hanover Sheriff's Office
16. Onslow County Sheriff's Office
17. Wayne County Sheriff's Office
18. North Carolina State Bureau of Investigations
19. Naval Criminal Investigative Service
20. USA Criminal Investigative Command
21. USAF Office of Special Investigations

Participating Federal agencies will include "OneDOJ" through R-DEx, and DHS through ICEPIC at a time to be determined by those entities and the NC Governance Board.

Subsequent phased expansion will be subject to resource availability and will seek to include *all* law enforcement entities from the Eastern North Carolina law enforcement community.

In addition to those participating entities listed above, the NC LInX Program will also seek to include connectivity with the Hampton Roads LInX and the National Capital Region LInX. All other agencies and data sources will be added at the discretion of the Governance Board, pending the availability of resources.

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

LInX builds on or leverages programs, networks and technical efforts existing or underway by enhancing those efforts and creating new information sharing capabilities, while fostering agreements between all of the participating agencies. For communities without

networks or organized information sharing efforts, LInX provides the help to put in-place the necessary information sharing infrastructure.

The technology that allows LInX users to gain access to the system relies on encrypted web-services between the agencies' users and the data warehouse.

The LInX System has introduce a unique concept that allows any records management system, or existing information sharing system to contribute to the data warehouse at a minimal impact to the agency's system. The unique capability is referred to as the front porch. The front porch is a special function that is established between a single, multiple or networked RMS and the data warehouse allowing all of the legally sharable RMS data to be standardized to NCIC standards and converted to the Global Justice XML Data Model (now referred to as the NEIM data model), then transferred to the data warehouse. This unique structure has greatly reduced the cost of interfacing any RMS to the data warehouse, making information sharing for law enforcement easy, affordable and secure.

6.3 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 uses in-place state-of-the-art information security tools to control access to law enforcement sensitive information, to include robust authentication, role-based security access levels and full auditing capabilities. Users will only be able to access information that they have been authorized to have access to.

6.4 What are the levels of access built into the LInX System?

Tactical Level - This level of access is provided to line or patrol officers, which allows 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 Level - This level of access is provided to criminal investigators and analysts to see all structured and free text source documents, conduct analysis on those documents and provide link analysis for the information contained therein.

Administrative / Security Level - This level of access is provided for system administrators as well as the security administrators for each participating agency.

Restricted / Sensitive / Task Force Level - This level of access will be developed to allow for a special isolated inclusion capability for very restricted information related to specialized task forces, highly sensitive investigations, and any investigative information that requires court authorization for disclosure (i.e. Federal Grand Jury, Title III, etc.).

All access to this level will be granted in writing by the Board, highly controlled and administered on a need to know basis only.

6.5 What are the access controls built into the LInX System?

Access to data and applications within the data warehouse is controlled using appropriate database management techniques. To insure data security, users will only perform an operation only if that user has been authorized to perform that operation. A privilege is an authorization to perform a particular operation; without privileges, a user cannot access

any information in the data warehouse. To ensure data security, users are only granted those privileges that they need to perform their specific job functions. A single user account can not be allowed to access the warehouse with more than one session at a time unless approved by an appropriately designated authority. Profiles can also be used to disable a user's session after a designated period of inactivity.

The system maintains tight control over which privileges a user is granted and under what conditions these privileges can be used. These features are used to enforce separation of duties based on user roles and responsibilities. They are also used to strictly limit access to the warehouse, its data, and applications in order to protect them from unauthorized access, disclosure, modification, or erasure.

The warehouse has the technical ability to restrict each user's access to only that information necessary for operations and for which the user has the need-to-know. Access control is implemented in such a way as to duplicate use restrictions within the participating agency's' source databases. Wherever possible, user roles and access restrictions are standardized across agencies. The data warehouse employs user certificates and has the capability to utilize PKI certificates.

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

Every effort is made to comply with all federal and state legal and regulatory requirements to include 28 CFR, FOIA, as well as making sure that any and all state privacy and confidentiality requirements are supported by this effort. Some of the issues that are being addressed include—secure storage of information, inquiry/search/ audit capability, controlled dissemination, public disclosure and the review and purge process.

Even though the system does not contain any level of intelligence data, the LInX System was built to be fully compliant with 28CFR Part 23.

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

The LInX System can ingest just about any and every records management system data format. It has collected and successfully ingested structured data, such as the data in many law enforcement records management systems—citations, incident reports, pointer systems, etc. It can also ingest many unstructured forms of data, such as those created during investigations—free text documents. LInX is using an open decoupled architecture and only 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 officers, investigators and analysts within the community.

6.8 What database management system does the LInX System use?

The current LInX System is built on an Oracle relational database management system (RDBMS).

6.9 What are the basic capabilities of the LInX System?

The basic capabilities that are delivered with the LInX System include:

- simple query, structured entity search (person, incident, vehicle, weapon),
- free text search,

- link analysis.

Additional enhancements and capabilities such as geospatial mapping may be added based on available funding, unique requirements, and in-general as the project matures.

6.10 Will all capabilities be available to all users?

No. Patrolman and other tactical level users will only have access to tactical query and structured entity searches which will return information on searched names, addresses, vehicles, phone numbers and incidents. Investigators and analysts will have access to all of the LInX capabilities based on the assigned roles.

6.11 What are link diagrams?

Link diagrams are used to create a visual depiction of the relationships between entities (people, addresses, vehicles, incidents, etc.) from the collected information in the data warehouse. The LInX effort currently includes the Adobe-SVG link analysis product which will assist investigators by uncovering, interpreting, and displaying complex information in easily-understood chart format.

The LInX Program can also support external special use link analysis programs such as i2 Analyst Notebook, Visual Analytics, etc.

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

The LInX data warehouse only requires a standard PC or similar capability, a web browser, high speed internet connectivity, and the appropriate access level assigned by the system administrator.

6.13 What is the data warehouse?

The LInX data warehouse is a centralized group of servers designed and formatted to facilitate tactical, investigative, strategic, and management decisions. It includes federal, state, county and municipal agencies' investigative and incident structured and free text data. The LInX warehouse consists 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, constraints, indexes, and relationships.
- Data Extraction and Transformation Tools – Tools that allow the warehouse to extract data from law enforcement records systems.
- 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 linkages 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 organized enterprises on crime in the area. 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 through the front porches.

6.14 What is meant by Auditing?

The LInX data warehouse includes an audit capability for the system and its users. The system logs all user actions to include time of user queries, actual queries executed, query results, alerts set, and notifications received. A permanent tape backup will be maintained in compliance with public disclosure, FOI and Privacy Act requirements for a period as prescribed by the laws, ordinances, policies and regulations of the participating agencies.

6.15 Will LInX Users have access to NCIC Criminal Histories?

The policies and configuration of the LInX Program does not permit access to the State Information Switch. As such, direct access to data bases such as NCIC, State DMV, Wants and Warrants, etc will not be available through the LInX System. If at a later date the Governance Board determines that access to the State Switch is appropriate (and concurred with through in-depth legal review), then access will be reconsidered, based on funding, legal and security review and acceptance.

Currently users of the LInX System undergo training for system use and do not undergo the appropriate training for obtaining NCIC certification (including the testing required for this certification). As such, any future consideration for allowing LInX users to access the State Information Switch would take this requirement into consideration.

6.16 Deconfliction

If the system contains all available legally sharable investigative and incident information for the participating law enforcement agencies within a region, then deconfliction for all levels of cases becomes a matter of policy. Without the use of LInX, deconfliction would be the result of personal knowledge of on-going regional activities or hit-or-miss phone calls to agencies in hopes of determining if another agency is working a similar case or on similar subjects.

As long as all of the available the RMS and investigative information has been at least indexed in the LInX data warehouse, a quick check of the system will revel at a minimum, a pointer to another investigation that could be active or provide supporting information. Directing these checks becomes a matter of policy for every participating agency making deconfliction easy and a normal course of business.

6.17 How will LInX be accessed?

The system will be accessed via the internet. Users and administrators currently access LInX using a browser that operates on both the public and/or private networks.

6.18 How is Access Security handled? *(Name and password or some type of VPN technology?)*

At a minimum:

- All users have a unique ID and password;
- System side certificates are in place in order to access the system (https);
- There are rules for session timeouts, lockouts, retries and password management;
- User to system interaction employs at least 256 bit encryption;
- System to system uses AES for encryption.

Also available:

- VPN's or other closed networks can be employed, but are not required;
- Strengthened passwords and PKI security can be added if required (pin + random number).