

OHIO ASSOCIATION OF CHIEFS OF POLICE

Local Law Enforcement Information-Sharing Network System Documentation



I. REVISION HISTORY

Date	Version Number	Description	Editor
8/24/2004	1.0.0	Initial Version	Brett Gerke
9/24/04	1.1	Revision to Give to Receive Policy, Date Staged Implementations, and Steering Committee Membership	Ted Oakley

II. TABLE OF CONTENTS

	<u>Page</u>
I. REVISION HISTORY	2
II. TABLE OF CONTENTS	3
III. INTRODUCTION	5
A. HISTORY	5
B. VISION AND GOAL	6
C. FOCUS GROUP RESEARCH	6
D. CENTRALIZED DATA REPOSITORY	7
E. SCOPE AND LEADERSHIP	8
F. REPORT ORGANIZATION	9
IV. SYSTEM OVERVIEW	11
A. GUIDING PRINCIPLES	11
B. DESIGN DECISIONS	15
V. SYSTEM DOCUMENTATION	21
A. FACILITIES	21
B. OPERATIONAL REQUIREMENTS	22
C. ENVIRONMENTS	23
D. PLATFORMS	23
E. NETWORK ARCHITECTURE	24
F. SAN AND DATABASE ARCHITECTURE	24
G. SECURITY ARCHITECTURE	25
H. SYSTEM ACCESS	26
I. INTERFACES	27

APPENDIX A – HIGH-LEVEL ARCHITECTURE DIAGRAMS

APPENDIX B – GLOBAL DATA ELEMENTS

APPENDIX C – LOCAL DATA ELEMENTS¹

APPENDIX D – STEERING COMMITTEE LISTING

APPENDIX E – GLOSSARY

APPENDIX F – DIAGRAM OF STAGING / RELEASE PROCEDURES

APPENDIX G – DIAGRAM OF OHLEG NETWORK ARCHITECTURE

APPENDIX H – DIAGRAM OF SAN AND DATABASE ARCHITECTURE

APPENDIX I – DIAGRAM OF SECURITY – USER ADMINISTRATION

¹ At this time, no local elements are enlisted.

I. INTRODUCTION

III. INTRODUCTION

The purpose of this living text is to document overall design, development, deployment and support of the Ohio Local Law Enforcement Information-Sharing Network (OLLEISN). It is a place to record current as well as strategic plans for the system. In some cases, placeholders have been included to assure clear and complete details are provided at a future date when decisions are made. It will be a place to record design decisions, and technical architectures as well as provide guidance for future development and support.

A. HISTORY

The terrorist attacks of September 11, 2001, demonstrated the need to proactively aggregate and analyze information. The devastating consequences of a few determined people might have been prevented if local, state, and federal law enforcement agencies had been able to quickly and efficiently coordinate, share, and analyze information. In the aftermath of this event, the federal government has begun to increase electronic information sharing between federal agencies and to gradually make this information more available to state and local law enforcement.

Equally important to public safety, and the war on terrorism, is the need for local law enforcement to share information during their day-to-day activities. Unfortunately, the capability to electronically share information between local law enforcement agencies does not exist. The vast majority of local law enforcement agencies in states, including Ohio, are not able to share electronically information from their records management systems (RMS) and computer-aided dispatch (CAD) systems with one another, and many do not have the ability to access state and federal crime databases. This lack of information sharing puts our communities, states, and nation unduly at risk. The series of highway shootings in the central Ohio area during the past year is an excellent example of this risk. Lacking a way to quickly and efficiently share record information with one another, the jurisdictions involved in the investigation of individual shootings did not perceive a pattern to the shootings until a homicide occurred.

B. VISION AND GOAL

The vision of the local law enforcement leaders in Ohio is to create a standards based information and communication network that links all 900+ local law enforcement agencies in the state by utilizing computer technology.

The goal is to provide local law enforcement officers with the information and communication abilities necessary to make the most accurate and timely street-level decisions by providing a common set of information to be shared by local law enforcement agencies under a secure infrastructure. The Ohio Association of Chiefs of Police, Inc. (OACP) is providing leadership for one aspect of this effort, the creation of OLLEISN, which will electronically share information stored in the RMS and CAD systems of Ohio local law enforcement agencies in a centralized data repository.

C. FOCUS GROUP RESEARCH

Early in the planning process, OLLEISN project leaders made strategic decisions to partner with CAD/RMS providers² to deliver a seamless interface for shared information. In order to initiate that partnership, OACP conducted a meeting with providers to present the vision of OLLEISN and seek their cooperation. Their responses, concerns and recommendations are available on the OACP project web site: <http://www.oacp.org/infoshare/vendor.html>

Overall results of this meeting were very encouraging.

- The providers attending wished to be included in the project at the earliest possible time.
- The providers were willing to work with their customers to determine the presentation and local processing of the shared information.
- The providers wanted to be kept abreast of all design and development efforts for the OLLEISN project. Some even wanted to actively participate in the design and development of the project.
- Providers not currently doing business in the State of Ohio also wanted to be included in all communications about the project, design decisions and implementation.

The project team responded to these requests and suggestions by providing complete communications and invitations to attend all design and development meetings for the project. All providers that expressed interest have been kept up-to-date on all design and implementation decisions as well as the ongoing status of the project.

² This term applies to any RMS or CAD service provider such as agencies that develop their own solution, vendor-provided solution or other consortium or service offering

Strategic planning sessions with local law enforcement executives were held in Columbus, Cleveland, Cincinnati and Toledo. Over five hundred executives attended to learn about the OLLEISN vision and to provide their insights and suggestions for the project. As with the providers, the executives were enthusiastic and fully supportive.

In addition to the strategic planning meetings with the CAD/RMS providers and law enforcement executives, focus group research sessions were conducted with street officers, investigating officers and executive officers. The results are available on the OACP project web site: <http://www.oacp.org/infoshare/news.html>

The results of this research disclosed:

- Street officers feel that too much information is as bad as too little information and that information presented must be clear and concise.
- Investigating officers need all the information that can be provided as long as it is accurate.
- Executive officers require the same information as street and investigative officers but in a summarized manner that allows them to perform their job duties.
- Each group found it important that we provide information that focused on all contacts an individual had with law enforcement. This included such items as:
 - » Arrest records
 - » Wants / Warrants
 - » Alerts, medical, psychological, etc...
 - » Field Interrogation / Interview Reports
- Critical to all groups was the ability to assure the true identity of a person.

The results of this research are being used to define the requirements of this project and the global data element set.

D. CENTRALIZED DATA REPOSITORY

After considering various alternatives for how Ohio local law enforcement agencies could effectively and efficiently share information with each other, the OLLEISN Steering Committee decided to utilize a centralized data repository containing filtered data uploaded from local CAD / RMS systems. They accepted the offer of Ohio Attorney General, Jim Petro to host the repository at the Attorney General's Ohio Law Enforcement Gateway (OHLEG) site.

E. SCOPE AND LEADERSHIP

The scope of the project encompasses information sharing between all local law enforcement agencies in Ohio. As discussed in the previous subsection, user research revealed that the project focus should be on the local law enforcement officer and investigator. Information gathered and shared at this level is normally summarized in order to be used by managing officers and executives.

The steering committee that is responsible for the oversight of this project as well as playing an advisory role for OHLEG is made up of select representatives from the following:

- Ohio Department of Public Safety (ODPS)
- Ohio Attorney General (OAG)
- Ohio Association of Chiefs of Police (OACP)
- Buckeye State Sheriffs' Association (BSSA)
- Ohio State Highway Patrol (OSHP)
- Office of Criminal Justice Services (OCJS)
- Mobile Area Radio Communication System (MARCS)
- Regional Information Systems

The current membership of the steering committee is included as APPENDIX D.

F. REPORT ORGANIZATION

In order to successfully convey the specific framework of OLLEISN to stakeholders, agencies, and CAD / RMS providers, this document will be expanded and maintained over the life of OLLEISN. While it draws on the strategic guiding principles and design decisions made for the entire state of Ohio, its focus is on the current architectural issues of OLLEISN.

The remainder of this document is organized as follows:

- Section II discusses the strategic guiding principles, design decisions, and any further discussion notes that frame this project.
- Section III outlines the technical architectures, designs, deployment and support details that will guide the development of OLLEISN.
- APPENDIX A presents high-level diagrams that describe the OLLEISN architecture.
- APPENDIX B lists the global data elements of the most recent model.
- APPENDIX C provides a listing of local data elements. This appendix will serve as a placeholder for the first iteration of this document. Local elements have not yet been defined for inclusion of the pilot project.
- APPENDIX D presents the OLLEISN steering committee roster.
- APPENDIX E provides a glossary.
- APPENDIX F is a diagram of the staging / release procedures
- APPENDIX G is a diagram of the OHLEG network
- APPENDIX H is a diagram of the Storage Area Network (SAN) and Database
- APPENDIX I is a diagram of the security - user administration

II. SYSTEM OVERVIEW

IV. SYSTEM OVERVIEW

This section presents an overview of the OLLEISN architecture, including:

- Guiding principles of the information-sharing solution.
- Specific decisions that affect the design of the information-sharing solution.
- Restrictions, constraints, and limitations to the architecture design.

A. GUIDING PRINCIPLES

In order to uphold the vision of this project and to ensure that the development direction of OLLEISN stays true to its goals and purposes, a series of guiding principles are needed. These principles, derived from the project's vision, goals, and purpose, have guided decisions already made about what information technologies to use and how they will be employed and will continue to guide all future decisions. These guiding principles are:

- Maintaining Local Law Enforcement Control

Ohio is a home-rule state; therefore, all agencies are able to choose their own CAD / RMS developer for automating their information systems. One of the main priorities of this project is to ensure that local law enforcement agencies maintain control of their in-house data. This will be accomplished by maintaining the opportunity for local law enforcement agencies to select CAD / RMS providers of their choice. This encourages participation by all local law enforcement agencies in the state.

- Common Components

Given the wide variety in technologies that exist in the environment of participating agency, a set of common components will be designed and developed for compatibility with various technologies. General categories of these common components are:

- » *System Load/Update* – responsible for the loading and updating of contributing agency information to OLLEISN. Initially this will be done in batch mode using FTP, strategically; we would like to see real-time updates via transactional information provided by the RMS systems through web services / SOAP.
- » *System Query* – handles agency inquiries and returns XML tagged result sets.
- » *Audit* – auditing transaction information, including information regarding the user, data, and time of transaction. These should follow the standards laid out by NCIC.
- » *Security* – assuring the authentication and authorization of all that access the system.

Agency's computerized information systems are to be able to access a shared database and select the needed data elements using a technology agnostic interface to these common components. This provides developers the control over the data to fulfill the needs of their customers. The requested information (found sets) is located via predefined stored procedures and returned in standard formats as a result of that query. Queried information will be able to be sorted by specified criteria. APPENDIX A presents a high level description of both the system load/update and system query functionality

- Voluntary Participation

Participation in this project is voluntary and operates in a manner that provides a certain amount of autonomy for each agency. Working within a framework of established statewide information-sharing standards, local law enforcement leaders keep the ability to decide how they maintain and operate their RMS and CAD systems. Participation in this system is necessary to assure inclusion of all information available.

- Policy of "Give to Receive"

We require that all agencies share a predefined minimum number of data fields to the system in order to be able to obtain information from the system. The steering committee will approve the minimum amount of information that will be shared by each participating agency. Information from all agencies is deemed valuable and will benefit all participants. OLLEISN is committed to assisting local law enforcement agencies desiring to share information to be able to do so.

- State Standards

Local agencies that have a computerized CAD / RMS systems use software provided by over 70 different providers. Working in partnership with these CAD / RMS providers, common network standards will be developed to allow the clients of all CAD / RMS providers in Ohio to share record information. In addition, software and technical standards will be developed to guide the procurement of computerized RMS for the estimated 40 percent of Ohio law enforcement agencies without one. Deviations from identified standards will be avoided, as they will create a significant short-term and/or long-term negative impact on efforts during implementation and maintenance of the system.

- National and Industry-Standard Protocols and Open Systems Technology

OLLEISN's design is based upon current and developing national standards, such as the Global Justice XML Data Model (GJXDM), and industry standards, such as web services

and SOAP to ensure compatibility with future technology and the ability of local law enforcement agencies to share information with other state and federal agencies in the future.

■ Security Standards and Best Business Practices for Security

A critical component to the OLLEISN architecture is the security environment. The shared information must be both secure and private and conform to all applicable public record laws and privacy rights. In order to best secure OLLEISN and meet all applicable security and privacy requirements, the architecture follows industry best practices. In addition, the security standards and best practices of stakeholder agencies are considered within the overall security design.

■ Robust Management Features for Access Control and Auditing

Management support for the OLLEISN environment is essential to success and acceptance of the project. Specific management capabilities include:

- » Managing and controlling access to all shared information.
- » Auditing information access at all points.

Auditing will be comprehensive for all upload and query access, however auditing at the data element level will not be supported.

■ Robust Operational Features for Error Handling, Debugging, and System Testing

Operational support for the OLLEISN environment is essential to the success of the project. Specific operational capabilities will include:

- » Monitoring technical performance including server loads and response times.
- » Reporting system and query failures in enough detail to support debugging.
- » A system for testing interfaces that enables visibility to system checkpoints.

These operational features minimize the level of effort required for error handling, troubleshooting, debugging, system testing, and overall maintenance.

■ Scalable Environment

OLLEISN's design must be scalable to support all local law enforcement agencies in Ohio, new requirements as they are identified and defined, and transaction volume increases. This includes support for introducing new extensions and software releases into existing operational environments. In addition, OLLEISN must be designed and developed in a way that offers the ability to expand functionality with minimal cost, time, and effort.

■ Data Standards

Data must be standardized to provide consistency of data definitions for all shared data. Initially, the standardized data sets include:

- » Arrests (not including booking information).
- » Cautions / Alerts.
- » Wants / Warrants.
- » Incident information from the Ohio Incident-Based Reporting System (OIBRS).³

The future vision is to support other data sets such as field interview reports. The statewide data model will provide for access, interoperability, and communication of this standardized data.

■ Data Ownership

Shared data will be provided on a read-only basis. The accuracy, quality, and purity of the information to be shared is the responsibility of the contributing agency. The steering committee will approve the minimum amount of information that will be shared by each participating agency. Dissemination of the shared data and all interfaces to the shared data must receive steering committee approval. Participating agencies must acknowledge this design decision early in implementation. In support of this principle, OLLEISN will not attempt to aggregate records or utilize any type of master name indexing solutions.

■ Architecture Deviations

Architecture deviations will be handled on a case-by-case basis, with emphasis on the cost of noncompliance and total value for deviation presented by the agency requesting the deviation. The burden of justification for exceptions is the responsibility of the requesting agency and/or CAD / RMS provider. Any architecture deviations will be managed and approved by the technical subcommittee before being presented to the steering committee. The steering committee must strongly consider the long-term architectural impact, as well as indirect effects that could be passed along to partner organizations, during the decision-making process.

■ Agency System Independence or Interchangeability (interface agnostic)

Architectural components will be designed, developed, and implemented to allow agencies to upgrade or replace RMS and CAD systems with minimal impact or disruption to the inter-

³ This will also include derived UCR information.

faces and no impact to the OLLEISN environment. This will remain an important principle as OLLEISN evolves to allow for easier support and operations.

- System Performance

To support quick access to information by patrol officers, the system must support fast response times for most queries. However, some queries that return more detailed information may require more time.

- Query Flexibility

Queries will enhance the information reporting capabilities of the agency systems. Many queries will be common across RMS and CAD systems. However, every system will have the flexibility to propose for testing and approval, their own queries to support the specific requirements of their agency or capabilities of their system. Once the queries have been approved and implemented they will become available to all participants of OLLEISN.

- Support Transparency

The project stakeholders are committed to accomplishing transparent data sharing within the state. This concept will allow solution users to seamlessly access information regardless of geographic point of interaction, thus creating the sense of transparency.

The remainder of this section describes design decisions as well as the limitations and framework that will complete the high-level solution architecture.

B. DESIGN DECISIONS

Strategic design decisions concentrate on setting the technology direction for OLLEISN based on the vision and guiding principles previously described. These decisions affect the infrastructure, development design, and technical support environment that will enable improved and more efficient information sharing across the state. The key design decisions for this project include the following:

- Implementation

We will be taking a stair step approach to the implementation of the system. Starting with a pilot group consisting of a small number of related agencies, geographically disbursed, and following with a number of cohort groups to control deployment impact.

» Pilot

As a stepping-stone to the OLLEISN solution described in the vision, a pilot project has been initiated with 11 agencies.

» Staged Implementation

Following this pilot project, the current schedule includes two more groups of agencies be deployed by January 31, 2005.

There is a need to control the number of agencies / users joining the system to assure performance and reliability. Therefore, it's planned to submit cohort groups, determine the approximate data volume increase and maximum number of users accessing the system for each group, and submit this information to the OHLEG systems managers. The OHLEG systems managers will determine the total impact on the system. When the system is deemed ready to accept the group, they will be provisioned on the system. This procedure will be repeated until all agencies are on the system.

■ GJXDM 3.x Compliance

All shared information follows the Global Justice XML Data Model (GJXDM) version 3.x recommended by the United States Department of Justice (DOJ). An XML schema for the state of Ohio showing the subset of the GJXDM plus all extensions necessary will be provided. Mapping of each participating agency's data to the shared data formats and standards is the responsibility of each provider. The global data elements that have been determined to be sharable by the project steering committee, along with their corresponding data type and data element description, are presented in APPENDIX B. Local elements, as they are developed, will be included in APPENDIX C.

■ Web Services

Desired data elements will be requested and retrieved via web services, SOAP and XML technologies. This provides an abstraction layer between OLLEISN and the agency systems that is standards-based, provider and product independent. By using web services, standard XML tagging of the information can be used by the developers to ease the manipulation and presentation of the data to the users. However, not all participating agencies will be able to utilize web services; thus, deviations will be accommodated on a tactical basis. OACP will be responsible for the creation of interfaces for these deviations to the standard .NET interface.

■ Physical Location

On a voluntary basis, information from participating agencies will be periodically collected into OLLEISN, which will be physically collocated with OHLEG in OAG's Columbus data center. The OHLEG support staff will be responsible for the storage, security, and connectivity to the shared information collected there.

■ Data Access

Data access will initially be limited to participating Ohio law enforcement agencies. Access to data will be accomplished via two separate interfaces.

- Integrated user interface developed by the agency's RMS / CAD provider.
 - Developed to have the same touch and feel of the agencies existing system.
- The OHLEG/Search Engine developed by the AGO.
 - Allows access to data from any Internet presence via a Web browser.

This maximizes the options available to local law enforcement and increases system availability.

■ Data Retention

Data retention will be the responsibility of the participating agencies. The retention of audit logs will be according to the steering committee's policy.

■ Queries

All queries will be stored procedures residing on the ORACLE database. There will be no ad hoc query access to the data repository.

» Standard Queries

NOTE: These standard Queries will be enhanced and documented as part of the Pilot design and implementation

Queries that are common across agencies will be implemented as standard queries using web services and stored procedures. The OLLEISN database will be optimized for these queries and a guaranteed response time will be provided for these queries in the OLLEISN service-level agreement (SLA).

» Custom Queries

Queries that are agency or system specific will be developed and executed as stored procedures that reside on the database. All custom queries will be approved by the AGO in conjunction with the technical subcommittee before they are developed, tested, tuned and implemented.

■ Certification

Each provider must successfully complete the first step of a two-step OLLEISN certification process to participate in the system. The two steps include:

(1) Successful meeting of all system requirements to load information onto the system accurately, efficiently, and automatically.

(2) Successful meeting of all system requirements for an integrated user interface to access, retrieve and display shared information in the OLLEISN database.

Until a provider can meet step (2), OLLEISN will make available to the provider a standard user interface.

Additional guiding principles and/or design decisions may be added as well as revisions to the ones listed above, in future revisions of this document. All proposed technical changes will be reviewed and evaluated by the technical subcommittee and OHLEG IT staff before submitted to the steering committee

Discussion Notes

The following discussion notes support the information presented in the previous sections:

- The overall structure of this document is designed to be easily maintained, flexible and promote documentation of future design decisions. At this time, there are a few known decisions in which short-term design for the pilot may differ from that of the future, strategic vision. The following table presents a high-level evolution path of these known decisions:

Decision	Short-Term	Long-Term
Data Content	Public record information	Inclusion of more sensitive information
Data Sets	Arrests, wants and/or warrants, cautions and/or alerts, and incident information from OIBRS	Addition of other person information, and field interview reports
Data Center	Columbus, Ohio, and London, Ohio, as cold site	Columbus, Ohio, and London, Ohio, as hot site by 2005
User Access	Law Enforcement Officer, System Administrator, Auditor	All roles as defined in section III-G Use of Certificates
Data Stores	Focus design on operational data store to support queries with quick response times (street officers)	Elaborate design to include secondary data store with data mining capabilities for queries with longer response times (investigators)
Data Load / Update	Performed as ‘mass loads’ on a periodic basis via FTP	Performed real-time via transactions from participating CAD / RMS systems via web services / SOAP

The discussion notes provide supplemental design guidance to the OLLEISN architecture design.

III. SYSTEM DOCUMENTATION

V. SYSTEM DOCUMENTATION

OLLEISN will be supported by an array of computerized systems, information-sharing services, and technology tools. This section focuses on OLLEISN's design, architectures, deployment, and support needs including hardware, operating systems, communications devices, operational requirements, interfaces, and management tools that create the computing and communication environment necessary to support OLLEISN. The elements that compose the OLLEISN system include:

- Facilities
- Operational Requirements
- Environments
- Platforms
- Network Architecture
- SAN Architecture
- Security Architecture
- System Access
- Interfaces

A. FACILITIES

The Ohio Attorney General, Jim Petro, has volunteered his facilities, infrastructure, and staff to maintain the central data repository for this project. The OHLEG framework is already in place in the Columbus, Ohio, data center and provides the benefits of a security system, communications infrastructure, and database system that are documented, tested, and operational. In addition, the London, Ohio, data center provides a geographically diverse failover site. The data centers include:

Columbus Data Center – Each OHLEG application has web servers on Windows 2003 Server platforms sitting behind a reverse web proxy. Once the user authenticates to the proxy using ORI number, user-id (to uniquely identify users) and password, the proxy validates the user's access to the specific OHLEG application using a Lightweight Directory Access Protocol (LDAP) database and automatically populates the login screen into the application. The application servers also validate access rights to the application in the LDAP database. Currently, there is one application server for each application. In the future, those applications that will have public access will move to separate public access web servers and those without public access will move to secured access web servers.

London Data Center – The London data center serves as a cold site. The Columbus, Ohio data center is currently protected with off-site backups. The current plans are to equip the London, Ohio data center to mirror the Columbus data center. The London data center will be a hot site by 2005. A business continuity plan is in progress (7/28/04).

B. OPERATIONAL REQUIREMENTS

The operational requirements of the OLLEISN system include staffing, availability and performance requirements.

1. Staffing Requirements

OLLEISN will be maintained by OHLEG staff. OHLEG staffing requirements will likely include the following:

- *Database Administrator (DBA)* – For the pilot, OHLEG may require a full-time DBA. As the system stabilizes, it will probably require only a fraction of a DBA full-time employee (FTE).
- *Developers* – For the pilot, the OLLEISN development staff will be provided by the OACP. For the long term, the OHLEG developers should be able to support incremental changes to the system in-house on an as-needed basis.
- *Operations* – During the pilot and following the rollout of OLLEISN to new agencies, the system will need to be monitored closely by operations staff. In the long term, operational requirements will be a fraction of an operator FTE.

2. Availability and Performance

OLLEISN will have strict availability and performance requirements to support officers in the field. This includes the following characteristics:

NOTE: Service Level Agreements for the system are to be determined by the steering committee and OHLEG before the pilot.

- Long-duration outages in excess of will not be acceptable.
- The availability level will be no less than .
- Response times for summary queries should not exceed a maximum response time of .

C. ENVIRONMENTS

The OLLEISN environments include the following:

- *Development and Test* – The development and test environments will be hosted and maintained at the OACP Dublin, Ohio, facility. The CAD / RMS providers will need remote access to build and test their interfaces.
- *Staging* – Microsoft Windows operating system does not support partitioning, therefore, there is only one run-time environment available in any server or server cluster. In order to update web applications in a Microsoft .NET, it is necessary to not install new releases on the same equipment as the current release. A staging environment will be used that mirrors the production environment and will be hosted at both the OAG Columbus, Ohio, and London, Ohio data centers. The staging environments will be two identical and parallel equipment sets in each center. One equipment set will be active (production) and the other inactive (in standby).
- *Production* – The production environment will be hosted at the OAG Columbus, Ohio data center with an identical environment in the London, Ohio data center. It is planned that in 2005 the London data center will be a hot site for the Columbus data center and will be used for failover and business continuance.
- *Migration / Upgrades* -- New versions of the .NET code will be applied to the inactive (standby) equipment set, tested for completeness and usability, and then the environments will be switched. The former production equipment set will become the inactive (standby) equipment set and vice versa. This will provide a ‘fail back’ solution for severe outages after version releases. The cycle repeats itself with all subsequent releases. (refer to APPENDIX F for a diagram)

D. PLATFORMS

The OLLEISN platforms include database and application servers. To ensure scalability, the database and application servers must be on separate systems. The servers include:

- *Database Server* – The OHLEG application databases are hosted on Oracle 10g, which will be distributed across three dual processor servers running SUSE Linux. The database will be replicated with three identical servers running at the London data center. The database servers will host other database instances as well. Using several existing RMS databases as a basis, an initial estimate suggests that OLLEISN database storage requirements are on the order of gigabytes. Given OHLEG’s capacity on its SAN, storage will not be a limiting factor. Assuming 1,000 agencies, 1 to 2 simultaneous users per agency and 1 user transaction per

minute on average, OLLEISN database transaction requirements are on the order of 1,000 to 6,000 transactions per minute on average or 5,000 to 15,000 transactions per minute at peak.

- *Application Server* – The application server environment will be Microsoft .NET Framework 1.1 implementing web services. All application servers will be in a cluster for high availability and performance / load balancing.
- *Web Server* – Microsoft IIS will be the host for all web services. These servers will be redundant for high availability and performance / load balancing.

E. NETWORK ARCHITECTURE

The network of the OHLEG framework consists of a Gigabit network backbone, which is connected to the Internet through the Department of Administrative Services (DAS) and protected by redundant Cisco PIX 520 firewalls. It should be noted that OHLEG is planning on moving to a dedicated Internet connection with redundant Cisco PIX 515 firewalls in the near future, which will make network capacity a non-issue.

Please refer to APPENDIX G DIAGRAM OF OHLEG NETWORK ARCHITECTURE

F. SAN AND DATABASE ARCHITECTURE

The main Columbus storage system consists of Hewlett-Packard (HP) EVA (Enterprise Virtual Array)-5000 storage frames which are connected in a multi-pathed SAN configuration using two switches and optical fiber channel to the servers. The SAN currently has a 13 TB capacity with 10 TB in use. The SAN can easily expand to 36 TB by adding more drives or up to 72 TB by using higher-density drives.

Please refer to APPENDIX H DIAGRAM OF SAN AND DATABASE ARCHITECTURE

G. SECURITY ARCHITECTURE

OHLEG already includes an LDAP-based authentication server that will easily support the estimated 30,000 law enforcement officers in the state. The Ohio Peace Officer Training Academy (OPOTA) maintains the official registry of officers in the state in a SQL database. The accounts are replicated to the OHLEG LDAP server using Novell DirXML. Chiefs/Sheriffs then grant access to OHLEG applications by sending a form to the OHLEG staff. A custom Web interface is then used to turn on access to each application as needed for each particular user. OHLEG is currently working with the Ohio State Highway Patrol to provide registry of officers since they are not included in the OPOTA database. OHLEG also has an established a registration system for non-sworn law enforcement personnel.

OLLEISN security includes the following architectural components:

- *User Authentication* – Users access OLLEISN through their local RMS or CAD system. Users log in to their local system, which then passes the agency ORI and the userid to OLLEISN for authorization.
- *User Access* – Access to information is currently either granted or not. Strategically, role-based, according to the rights granted by the chiefs in their agencies is desired. Under role-based authorization, users may be assigned one or many roles. However, roles will be shared across agencies. For example, all users with the “patrol officer” role will have access to the same data. There will be separate access authorization for administrators and auditors of the system.
- *Upload / change access* – The RMSs will connect through the OHLEG virtual private network (VPN), which restricts access to the IP address of the RMS via FTP.
- *Physical Security* – The data center is protected by proximity sensors and thumbprint access required for access to the storage system.

Please refer to APPENDIX I – DIAGRAM OF SECURITY – USER ADMINISTRATION

H. SYSTEM ACCESS

The table below presents a summary of the system access information including user roles, statements of roles, and role-based access levels that OLLEISN may support in the future.

Users Roles	Statement of Roles	Role-Based Access Levels
Law Enforcement Executives	Grant access to data	Read-only to data with access-granting rights
Patrol Officers and Dispatchers	Retrieve critical data on an individual quickly	Read-only. Patrol officers will use mobile data terminals (MDTs) to access the system, and dispatchers will access the data for patrol officers without MDTs
Detectives/Investigators	Retrieve all information available on an individual (not time-critical)	Read-only
Law Enforcement Clerks	Occasionally assist patrol officers	Read-only but more limited than patrol officers and detectives
System Administrators/DBAs	Monitor and maintain the system including database tuning	Full administrative but access is controlled through policy and audits
Auditors	Establish the need of police chiefs to query on all data access, including information regarding the user, data, and time stamp	Audit access. <i>NOTE:</i> The steering committee needs to determine a policy for selecting users with audit access privileges
CAD / RMS Systems	Incremental updates to OLLEISN. <i>NOTE:</i> Columbus and Mason are the only two pilot sites with separate RMS and CAD systems and may need interfaces from both systems	Write/update access to their agency data

I. INTERFACES

There are four identified interface components to OLLEISN, as described below.

1. CAD / RMS Upload Interface

This component must be based on open protocols. The CAD / RMS will push the data up to the repository using a standard format via FTP. The long-term design calls for transaction driven real-time updates via web services and SOAP.

2. CAD / RMS Query Interface to the Application Server

NOTE: The Query Interface will be detailed by the design of the common components and the .NET system for the pilot.

This component must also be based on open protocols, such as SQL, XML, or web services. It will likely be implemented in the short term to return XML-tagged data, with XML tags that are based on GJXDM 3.x. The long-term design calls for web services. This interface will support the following two types of queries:

- *Standard queries*, which have the following characteristics:
 - » Person-based.
 - » Quick, guaranteed response time.
 - » Primarily used for matches by identifiers which represent most of the transactions.
 - » An optimized database.
 - » Shared by most agency interfaces.
 - » Implemented as web services.
- *Custom queries*, which have the following characteristics:
 - » Can be requested by CAD / RMS providers.
 - » Are flexible to the needs of each CAD or RMS system.
 - » Can return detailed result sets as needed.
 - » Allow fuzzy-search matches.
 - » Implemented as web services.

3. Logging Interface

This interface component will serve auditors and executives and should be based on a standard format.

4. OHLEG/SE Interface

This interface will be developed and maintained by the AGO for authenticated browser based searches/queries over the Internet. Only OLLEISN participants with a valid OHLEG user account will be allow to utilize this feature. The security level will be identical to the access allow by the agency's RMS / CAD system.

* * * * *

The OLLEISN architecture will evolve over time to support the sharing of more information among more agencies. This document provides an initial framework for that architecture which is designed to satisfy the immediate requirements of the current pilot as well as the long-term information-sharing requirements of the law enforcement agencies across Ohio.

APPENDIX A
HIGH-LEVEL ARCHITECTURE DIAGRAMS

HIGH-LEVEL ARCHITECTURE DIAGRAMS

There are two aspects to the overall OLLEISN design: the information uploads and access to the information repository. The following subsections describe the available processes.

A. UPLOAD PROCESSES

The upload process diagrammed in this subsection represents the system load/update controlled by the common component standard defined in the main document. The normal update process will be a nightly or more frequent data load to the OHLEG repository with the overall goal being a near “real-time” data synchronization. “Real-time” data synchronization will require incremental and/or change log processes to be developed.

On a periodic basis, a predefined minimum number of data fields will be uploaded to the OHLEG repository.



B. INFORMATION ACCESS

The information access process diagrammed in this subsection represents the system query common component standard defined in the main document. The direct query method will be accomplished by the actions depicted in the steps below.

Step 1

The query request is sent from the agency's system to the OHLEG repository.



Step 2

Information in the repository that matches the query request will be returned to the requesting agency's system.



The agency's system will handle the presentation and display of the query results returned by the OHLEG Repository.

APPENDIX B
GLOBAL DATA ELEMENTS

XML SCHEMA		DATABASE PHYSICAL TABLE - ELEMENTS			DEFINITIONS
<u>EnforcementOfficial</u>	<u>EnforcementOfficialType</u> <u>extends PersonType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A person involved in the enforcement of law. This generally refers to a person designated by a public authority to keep the peace and arrest persons guilty or suspected of crime. May include, but not limited to: police, sheriff, marshal, federal authorities, military.
EnforcementOfficialType Text	TextType	ENFORCEMENT_ OFFICIAL	TYPE	VARCHAR2 (30)	A type of enforcement official, e.g., Detective, Investigator, etc.
EnforcementOfficial BadgeID	IDType extends SuperType	ENFORCEMENT_ OFFICIAL	BADGE_ID	VARCHAR2 (10)	An identifier used to refer to an enforcement official.
EnforcementOfficialUnit	EnforcementUnitType extends OrganizationType	ORGANIZATION	N/A	N/A	An enforcement unit to which an enforcement officer is assigned, e.g., patrol, detective, narcotic.
<u>Person</u>	<u>PersonType</u> <u>extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Describes inherent and frequently associated characteristics of a person.
PersonType	TextType	PERSON	PERSON_TYPE	VARCHAR2 (15)	Type of person (e.g. SUBJECT).
PersonName PersonAlternateName PersonAlias	PersonNameType extends SuperType	PERSON_NAME	PERSON_NAME_ CD (PRI) PERSON_NAME_ CD (ALT) PERSON_NAME_ CD (ALI)	VARCHAR2 (10)	A name by which a person is known: primary name (PRI); alternative name (ALT); alias name (ALI).
PersonPrefixName	TextType	ENFORCEMENT_ OFFICIAL PERSON_NAME	PREFIX_NAME	VARCHAR2 (10)	A title or honorific used by a person, e.g., Dr., Judge, General, Ms.
PersonGivenName	PersonNameTextType extends TextType	ENFORCEMENT_ OFFICIAL PERSON_NAME	FIRST_NAME FIRST_GIVEN_NAME	VARCHAR2 (20)	A first name of a person.
PersonGivenName Soundex	PersonNameTextType extends TextType	PERSON_NAME	FIRST_GIVEN_NAME_ SOUNDEX	VARCHAR2 (20)	A first name of a person using soundex.
PersonMiddleName	PersonNameTextType extends TextType	PERSON_NAME	MIDDLE_NAME	VARCHAR2 (20)	A middle name of a person.
PersonSurName	PersonNameTextType extends TextType	ENFORCEMENT_OFFICIAL PERSON_NAME	LAST_NAME SURNAME	VARCHAR2 (30)	A last name or family name of a person.
PersonSurNameSoundex	PersonNameTextType extends TextType	PERSON_NAME	SURNAME_SOUNDEX	VARCHAR2 (30)	Last name or family name of a person using soundex.

PersonSuffixName	TextType	PERSON_NAME	SUFFIX_NAME	VARCHAR2 (20)	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, e.g., Jr, Sr, III, or otherwise qualifies the name (e.g., MD, LLD, PhD).
PersonMaidenName	PersonNameTextType extends TextType	PERSON_NAME	MAIDEN_NAME	VARCHAR2 (20)	An original surname of a person before changed by marriage.
PersonMaidenName Soundex	PersonNameTextType extends TextType	PERSON_NAME	MAIDEN_NAME_SOUNDEX	VARCHAR2 (20)	An original surname of a person before changed by marriage using soundex.
PersonFullName	PersonNameTextType extends TextType	ENFORCEMENT_OFFICIAL PERSON_NAME	FULL_NAME	VARCHAR2 (70)	A complete name of a person.
PersonMiddleInitial	TextType	ENFORCEMENT_OFFICIAL PERSON_NAME	NAME_INTIAL MIDDLE_INTIAL	CHAR(1)	A first letter of a person's given, possibly middle, and last names.
PrimaryContactInformation	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (1)	N/A	Information on a preferred or primary contact mechanism.
PersonDayContact	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (2)	N/A	The contact information should be used during daylight hours only.
PersonEveningContact	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (3)	N/A	The contact information should be used during evening hours (early night) only.
PersonAuditTrail	AuditTrail Type	PERSON	N/A	N/A	An individual or organization can track their record/transaction.
PersonResidence	PersonResidenceType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	A set of details about identifications issued to a person.
Residence	ResidenceType extends LocationType				Details about the place in which a person lives.
ResidenceTypeText	TextType	ADDRESS	RESIDENCE_DESCR	VARCHAR2 (30)	A type of place at which a person lives, e.g., house, apartment, homeless.
ResidenceStartDate	j-xsd:date	ADDRESS	RESIDENCE_START_DATE	DATE	A date a person began living at a residence.
ResidenceEndDate	j-xsd:date	ADDRESS	RESIDENCE_END_DATE	DATE	A date a person stopped living at a residence.
PersonDetails	PersonDetailsType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	A set of details about identifications issued to a person.
PersonBirthDate	j-xsd:date	PERSON	BIRTH_DATE	DATE	A date a person was born.
PersonAgeMeasure.Range	RangeAgeMeasureType extends RangeMeasureType	PERSON	RANGE_FROM_AGE RANGE_TO_AGE	NUMBER (3)	A measurement of the age of a person.

<u>PersonAssignedIDDetails</u>	<u>PersonAssignedIDDetails</u> <u>Type</u> <u>extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element</u> <u>Name</u>	<u>Physical Element</u> <u>Data Type</u>	A set of details about identifications issued to a person.
PersonSSNID	IDType extends SuperType	PERSON	SSN	VARCHAR2 (11)	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of a person. Sometimes referred to as a SSN.
PersonDriverLicenseID	DrivingJurisdictionAuthority IDType extends IDType	PERSON	DRIVER_LICENSE_ NUMB	VARCHAR2 (15)	Information about an identifier used to refer to a specific person who has obtained a driver's license. Sometimes referred to as driver license number, dlNumber.
DrivingJurisdictionAuthority Code	j-ansi_d20:Jurisdiction AuthorityCodeType	PERSON	DRIVING_JRSDCTN_ AUTHORITY_CD	VARCHAR2 (2)	A federal or state organization, such as a department of motor vehicles (DMV), with jurisdiction over a person's driving privileges.
<u>PersonPhysicalDetails</u>	<u>PersonPhysicalDetails</u> <u>Type</u> <u>extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element</u> <u>Name</u>	<u>Physical Element</u> <u>Data Type</u>	A set of details about the physical appearance of a person.
PersonHeightMeasure. Range	RangePersonHeight MeasureType extends RangeMeasureType	PERSON	RANGE_FROM_ HEIGHT RANGE_TO_HEIGHT	VARCHAR2 (15)	A measurement of the height of a person.
PersonWeightMeasure. Range	RangePersonWeight MeasureType extends RangeMeasureType	PERSON	RANGE_FROM_ WEIGHT RANGE_TO_WEIGHT	VARCHAR2 (15)	A measurement of the weight of a person.
PersonEyeColorCode	j-ncic:EYEType	PERSON	EYE_COLOR_CD	VARCHAR2 (10)	A code identifying the color of a person's eyes.
PersonHairColorCode	j-ncic:HAIType	PERSON	HAIR_COLOR_CD	VARCHAR2 (10)	A code identifying the color of a person's hair.
PersonSexCode	j-ncic:SEXTYPE	PERSON	SEX_CD	VARCHAR2 (10)	A code identifying the gender or sex of a person.
PersonRaceCode	j-ncic:RACType	PERSON	RACE_CD	VARCHAR2 (10)	A code identifying the race of a person.
PersonPhysicalFeature	PhysicalFeatureType extends SuperType	PERSON_PHYSICAL_ FEATURES	N/A	N/A	Details about a physical feature of a person. Includes scars, marks, and tattoos.
PhysicalFeatureCategory Text	TextType	PERSON_PHYSICAL_ FEATURES	PHYSICAL_ FEATURES_ CATEGORY	VARCHAR2 (20)	A general classification or categorization of a physical feature, e.g., scar, mark, tattoo, missing limb.
PhysicalFeatureTypeText	TextType	PERSON_PHYSICAL_ FEATURES	SCAR_MARK_TATOO_ DESCR	VARCHAR2 (50)	A type of physical feature within a category, e.g., for a tattoo type, this

					could be animal, flag.
PhysicalFeatureTypeCode	j-ncic:SMTType	PERSON_PHYSICAL_FEATURES	SCAR_MARK_TATOO_CD	VARCHAR2 (10)	A code identifying a type of physical feature.
PhysicalFeatureLocationText	TextType	PERSON_PHYSICAL_FEATURES	SCAR_MARK_TATOO_LOCATION	VARCHAR2 (20)	A location of a physical feature on a person's body.
<u>PersonSocialDetails</u>	<u>PersonSocialDetailsType extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A set of details about the social characteristics of a person.
PersonEthnicityCode	j-nibrs:EthnicityCodeType	PERSON	ETHNICITY_CD	VARCHAR2 (10)	A code identifying a person's cultural lineage.
PersonCitizenshipCode.fips 10-4	j-fips_10-4:CountryCodeType	PERSON	CITIZENSHIP_CD_FIP S104	VARCHAR2 (10)	A code identifying a country that assigns rights, duties, and privileges to a person due to the person's birth or naturalization in that country.
PersonCitizenshipCode.iso 3166Numeric	j-iso_3166:CountryNumeric CodeType	PERSON	CITIZENSHIP_CD_ISO 3166N	VARCHAR2 (10)	A code identifying a country that assigns rights, duties, and privileges to a person due to the person's birth or naturalization in that country.
PersonUSCitizenIndicator	j-xsd:boolean	PERSON	US_CITIZENSHIP_INDIC	BIT	True if a person is a citizen of the United States; false otherwise.
PersonNationalityCode.fips 10-4	j-fips_10-4:CountryCodeType	PERSON	NATIONALITY_CD_FIP S104	VARCHAR2 (4)	A code identifying the country in which a person was born.
PersonNationalityCode.iso3 166Numeric	j-iso_3166:CountryNumeric CodeType	PERSON	NATIONALITY_CD_IS O366N	VARCHAR2 (4)	A code identifying the country in which a person was born.
PersonMaritalStatus	TextType	PERSON	MARITAL_STATUS	VARCHAR2 (15)	A code identifying marital status of a person, e.g., married, divorced, single, separated.
<u>Subject</u>	<u>SubjectType extends PersonType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A person who is involved or suspected of being involved in an incident or criminal activity. This person may be the focus of an investigation or legal process, but is not necessarily the sole or primary focus.
SubjectIndicator	j-xsd:boolean	PERSON	WARRANT_INDIC ARREST_INDIC CHARGE_INDIC ALERT_INDIC	BIT	True if a warrant, arrest, charge, alert is present; false otherwise. Using boolean: a proxy structure that represents binary-valued logic (true/false).

SubjectContactInformation	ContactInformationType extends SuperType	CONTACT_PHONE_ EMAIL	N/A	N/A	The subject's contact information (e.g. phone, cell, pager, email).
---------------------------	---	-------------------------	-----	-----	--

DATABASE PHYSICAL TABLE - ELEMENTS					DEFINITIONS
<u>EnforcementUnit</u>	<u>EnforcementUnitType</u> <u>extends</u> <u>OrganizationType</u>	<u>Physical Table Name</u>	<u>Physical Element</u> <u>Name</u>	<u>Physical</u> <u>Element</u> <u>DataType</u>	Details about a unit of an agency responsible for enforcing the law and maintaining peace.
EnforcementUnitName	TextType	ORGANIZATION	UNIT_NAME	VARCHAR2 (30)	A name of an enforcement unit.
EnforcementUnitID	IDType extends SuperType	ORGANIZATION	UNIT_ID	VARCHAR2 (20)	An identifier of an enforcement unit.
EnforcementUnitSection ID	IDType extends SuperType	ORGANIZATION	UNIT_SECTION_ID	VARCHAR2 (20)	A section of an enforcement unit.
EnforcementUnitSection Name	TextType	ORGANIZATION	UNIT_SECTION_ NAME	VARCHAR2 (30)	A section name of an enforcement unit.
<u>Organization</u>	<u>OrganizationType</u> <u>extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element</u> <u>Name</u>	<u>Physical</u> <u>Element</u> <u>DataType</u>	Details about a unit which conducts some sort of business or operations.
OrganizationName	TextType	ORGANIZATION	NAME	VARCHAR2 (40)	A name of an organization.
OrganizationID	IDType extends SuperType	ORGANIZATION	ORGANIZATION_ID	VARCHAR2 (15)	An identifier of an organization based on the type of organization it is, e.g., for a school, this would be a school identifier, for a lien holder, this would be a lien holder identifier, for a court, this would be a court identifier.
OrganizationORIID	IDType extends SuperType	ORGANIZATION	ORI_ID	VARCHAR2 (10)	A unique identifier assigned to a justice-related organization by the federal government. Sometimes referred to as ORI, ORI code, Originating Agency Code.
OrganizationTypeCode.n cicORIAgency	j-ncic:ORIAgencyType	ORGANIZATION	ORI_AGENCY_ TYPE	VARCHAR2 (10)	A code that identifies the functional type of an organization.

OrganizationTypeCode.n cicTYPO	j-ncic:TYPOType	ORGANIZATION	FUNCTIONAL_TYPE_ NCIC TYPO	VARCHAR2 (10)	A code that identifies the functional type of an organization.
OrganizationLocation	LocationType extends SuperType	LOCATION	N/A	N/A	A location of an organization.
PrimaryContactInformation	ContactInformationType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_CD (1) This value will retrieve the primary phone number(s).	N/A	Information on a preferred or primary contact mechanism.
OrganizationGovernment LevelCode	j-ncic:ORIGovernmentLevel Type	ORGANIZATION	GOVERNMENT_ LEVEL_CD	VARCHAR2(4)	A code that identifies a governmental level of an organization: local, county, state, federal, or nongovernmental.
OrganizationDoingBusiness AsName	TextType	ORGANIZATION	DOING_BUISNESS_ AS_NAME	VARCHAR2(30)	A name an organization uses for conducting business. Sometimes referred to as a DBA.
OrganizationUnitID	IDType extends SuperType	ORGANIZATION	UNIT_ID	VARCHAR2 (20)	An identifier of an enforcement unit.
OrganizationUnitName	TextType	ORGANIZATION	UNIT_NAME	VARCHAR2(20)	A name of a high-level division of an organization, e.g., department, agency.
OrganizationUnitSectionID	IDType extends SuperType	ORGANIZATION	UNIT_SECTON_ID	VARCHAR2 (20)	A section of a unit.
OrganizationSubunitName	TextType	ORGANIZATION	SUB_UNIT_NAME	VARCHAR2(20)	A name of a subdivision of a high-level division of an organization, e.g., division.
OrganizationUnitBeatID	IDType extends SuperType	ORGANIZATION	UNIT_BEAT_ID	VARCHAR2(20)	A local area for which an enforcement unit is responsible.
OrganizationActivityText	TextType	ORGANIZATION	ACTIVITY_DESCR	VARCHAR2(50)	An activity that an organization is known or thought to be involved with, e.g., law enforcement, supervision.
OrganizationStatusText	TextType	ORGANIZATION	STATUS	VARCHAR2(15)	An overall status of an organization, e.g., active/inactive/...
OrganizationPrincipal Official	PersonType extends SuperType	ENFORCEMENT_ OFFICIAL	FULL_NAME	VARCHAR2(70)	A chief or high ranking executive of an organization.
OrganizationBranchName	TextType	ORGANIZATION	BRANCH	VARCHAR2(30)	A name or number of the chapter or branch an organization is known by within a larger group of organizations.
OrganizationPrimary Contact	ContactInformationType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_CD (1 = Primary)	N/A	The preferred contact for an individual. Use this designation only when more specific ones (e.g. home

					or work) are not available.
OrganizationDayContact	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (2= Day)	N/A	The contact information that is valid during daytime hours.
OrganizationEveningContact	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (3 = Evening)	N/A	The contact information that is valid during evening (early night) hours.
OrganizationUnspecifiedContact	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	CONTACT_CD (4= Unspecified)	N/A	The contact information should be used to contact the person under unspecified circumstances.
OrganizationAuditTrail	AuditTrail Type	ORGANIZATION	N/A	N/A	An individual or organization can track their record/transaction.

		DATABASE PHYSICAL TABLE - ELEMENTS			DEFINITIONS
<u>Address</u>	AddressType extends SuperType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A postal location to which paper mail can be directed.
AddressFullText	TextType	ADDRESS	ADDRESS_FULL	VARCHAR2 (50)	A complete address to be used when the address components cannot be broken down into the JXDD components.
Building	BuildingType extends SuperType	ADDRESS	N/A	N/A	Details about a building at a location.
BuildingFullText	TextType	ADDRESS	BUILDING_FULL	VARCHAR2 (50)	A complete reference that identifies a building.
BuildingName	TextType	ADDRESS	BUILDING_NAME	VARCHAR2 (20)	A name of a building, e.g., "Electronic Research Building"
BuildingNumberText	TextType	ADDRESS	BUILDING_NUM	VARCHAR2 (20)	A number or text associated with a building, e.g., 115C.
BuildingSubUnitText	TextType	ADDRESS	BUILDING_SUBUNIT	VARCHAR2 (30)	A department, group, division, or other subcomponent of a building.
Street	StreetType extends SuperType	ADDRESS	N/A	N/A	Details about a street.
StreetFullText	TextType	ADDRESS	STREET_FULL_	VARCHAR2 (30)	A complete street reference,

			REFERENCE		e.g., "123 Main Street NW".
StreetNumberText	TextType	ADDRESS	STREET_NUM	VARCHAR2 (10)	A number that identifies a particular unit or location within a street.
StreetNameText	TextType	ADDRESS	STREET_NAME	VARCHAR2 (30)	A name of a street.
StreetTypeText	TextType	ADDRESS	STREET_TYPE	VARCHAR2 (15)	A type of street, e.g., Street, Boulevard, Avenue, Highway, etc.
StreetPostDirectionalText	TextType	ADDRESS	STREET_POST_DIRECTIONAL	VARCHAR2 (20)	A direction that appears after a street name.
StreetExtensionText	TextType	ADDRESS	STREET_EXTENSION	VARCHAR2 (20)	Any additional parts of a street name that follows the street type and post directional.
AddressSecondaryUnitText	TextType	ADDRESS	SECONDARY_UNIT	VARCHAR2 (20)	A piece of information used to identify a particular unit within a specific location. Examples of this could be an apartment number or a suite number.
AddressRouteName	TextType	ADDRESS	ROUTE_NAME	VARCHAR2 (20)	The name and number of a postal route.
AddressCityName	TextType	ADDRESS	CITY_NAME	VARCHAR2 (20)	A name of a city or town.
AddressCountyName	TextType	ADDRESS	COUNTY_NAME	VARCHAR2 (20)	A name of a county, parish, or vicinage.
AddressCountyCode	j-fips_6-4:USCountyCodeType	ADDRESS	COUNTY_CD	VARCHAR2 (10)	A code identifying a county, parish, or vicinage.
AddressStateName	TextType	ADDRESS	STATE_NAME	VARCHAR2 (20)	A name of a state, commonwealth, province, or other subregion of a country.
AddressStateCode.CanadianProvince	j-can:CanadianProvinceCodeType	ADDRESS	STATE_CD_CANDIAN_PROV	VARCHAR2 (10)	A code identifying a state.
AddressStateCode.fips10-4International	j-fips_10-4:InternationalStateCodeType	ADDRESS	STATE_CD_FIPS_INTERNTL	VARCHAR2 (10)	A code identifying a state.
AddressStateCode.USPostalService	j-usps:USStateCodeType	ADDRESS	STATE_CD_US_POSTAL_SEV	VARCHAR2 (10)	A code identifying a state.
AddressPostalCodeID	IDType extends SuperType	ADDRESS		VARCHAR2 (10)	A zip code or postal code.
AddressPostalCodeExtensionID	IDType extends SuperType	ADDRESS	POSTAL_CODE_EXTENSION	VARCHAR2 (10)	An extension of a zip code or postal code.
AddressCountryName	TextType	ADDRESS	COUNTY_NAME	VARCHAR2 (20)	A name of a country.

AddressCountryCode.fips10-4	j-fips_10-4:CountryCodeType	ADDRESS	COUNTRY_CD_FIPS	VARCHAR2 (5)	A code that identifies a country, territory, or dependency.
AddressCountryCode.iso3166Numeric	j-iso_3166:CountryNumericCodeType	ADDRESS	COUNTRY_CD_ISO	VARCHAR2 (5)	A code that identifies a country, territory, or dependency.
Highway	HighwayType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	Details about a major public road.
HighwayID	IDType extends SuperType	LOCATION	HIGHWAY_ID	VARCHAR2 (10)	An identifier of a highway, e.g., "SR-78"
HighwayFullText	TextType	LOCATION	HIGHWAY_FULL_REFERENCE	VARCHAR2 (30)	A complete reference to a highway.
HighwayName	TextType	LOCATION	HIGHWAY_NAME	VARCHAR2 (20)	A name of a highway, e.g., "Stone Mountain Parkway"
HighwayPositionText	TextType	LOCATION	HIGHWAY_POSITION	VARCHAR2 (30)	A designation of a specific place on a highway. Sometimes referred to as a mile marker, mile post, exit number.
Location	LocationType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	Details about a physical location.
LocationName	TextType	LOCATION	LOCATION_NAME	VARCHAR2 (20)	A name of a location.
LocationTypeText	TextType	LOCATION	LOCATION_TYPE_DESCR	VARCHAR2 (30)	A functional description of a location, e.g., residence, school, agency, park.
LocationTypeCode	j-nibrs:LocationTypeCodeType	LOCATION	LOCATION_TYPE_CD	VARCHAR2 (10)	A code identifying a functional description of a location, e.g., residence, school, agency, park.
LocationAddress	AddressType extends SuperType	ADDRESS	N/A	N/A	Details about a postal address for a location.
LocationContactInformation	ContactInformationType extends SuperType	CONTACT_PHONE_EMAIL	N/A	N/A	Details about contact information for a location.
LocationHighway	HighwayType extends SuperType	LOCATION	N/A	N/A	Details about a major public road at a location.
LocationLandmarkText	TextType	LOCATION	LANDMARK	VARCHAR2 (30)	A name or description of a distinguishing physical feature at a location.
LocationAuditTrail	AuditTrail Type	LOCATION	N/A	N/A	An individual or organization can track their record/transaction.

		DATABASE PHYSICAL TABLE - ELEMENTS			DEFINITIONS
<u>ContactInformation</u>	ContactInformationType extends SuperType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element Data Type</u>	Details about how to contact a person or an organization.
ContactPerson	PersonType extends SuperType	PERSON	N/A	N/A	A person with the given contact information.
ContactPerson DescriptionText	TextType	CONTACT_PHONE_ EMAIL	PERSON_ROLE_ DESCR	VARCHAR2 (40)	A description of the title or function of a person with this contact information, e.g., Director of Public Relations, mother.
ContactTelephone Number	TelephoneNumberType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_PHONE_ CD (1)	N/A	A telephone number (contact phone code = 1) of a person or organization.
ContactPagerNumber	TelephoneNumberType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_PHONE_ CD (3)	N/A	A pager number (contact phone code = 2) of a person.
ContactMobile TelephoneNumber	TelephoneNumberType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_PHONE_ CD (2)	N/A	A mobile phone or cell phone number (contact phone code = 3) of a person.
ContactEmailID	IDType extends SuperType	CONTACT_PHONE_ EMAIL	CONTACT_PHONE_ CD (4) EMAIL_ID	VARCHAR2 (40)	An email address (contact phone code = 4) of a person or organization.
ContactMailingAddress	AddressType extends SuperType	ADDRESS	N/A	N/A	A mailing address of a person or organization.
ContactOrganization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	An organization at the site of the contact. Example: the organization that "owns" the physical telephone being called.
ContactAuditTrail	AuditTrail Type	CONTACT_PHONE_ EMAIL	N/A	N/A	An individual or organization can track their record/transaction.
<u>TelephoneNumber</u>	TelephoneNumberType extends SuperType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element Data Type</u>	Details about a number to be dialed to reach a contact.
TelephoneNumberFullID	j-xsd:string	CONTACT_PHONE_ EMAIL	FULL_NUM	VARCHAR2 (20)	A full length telephone identifier to be used when a number cannot be broken down into its subcomponents.
TelephoneAreaCodeID	j-xsd:string	CONTACT_PHONE_ EMAIL	AREA_CD_ID	VARCHAR2 (5)	A dialing code for a state or province for phone numbers in the USA, Canada, Mexico, and the Caribbean.

TelephoneExchangeID	j-xsd:string	CONTACT_PHONE_EMAIL	EXCHANGE_ID	VARCHAR2 (40)	The first three digits of a base telephone number. Usually represents a central telephone switch.
TelephoneSubscriberID	j-xsd:string	CONTACT_PHONE_EMAIL	SUBSCRIBER_ID	VARCHAR2 (5)	The last four digits of a base telephone number. Identifies the individual circuit within an exchange.
TelephoneSuffixID	j-xsd:string	CONTACT_PHONE_EMAIL	SUFFIX_ID	VARCHAR2 (10)	Additional numbers to be entered to direct a call to the appropriate place. Includes extensions, answering system navigation codes, and PINs.

DATABASE PHYSICAL TABLE - ELEMENTS					DEFINITIONS
<u>Event</u>	<u>EventType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A structure that describes details about a singular occurrence.
EventName	<u>TextType</u>	EVENT	NAME	VARCHAR2 (20)	A name of the event that occurred (e.g. OLLEISN Document Upload)
EventSequenceID	<u>IDType</u> <u>extends SuperType</u>	EVENT	SEQUENCE_ID	VARCHAR2 (15)	A sequence identifier of an OLLEISN Update occurrence.
EventSourceTypeText	<u>TextType</u>	EVENT	SOURCE_TYPE	VARCHAR2 (15)	A type or classification of an OLLEISN Document Upload event that occurred: ALRT (alert), WRNT (warrant), ARST (Arrest), CHRG (Charge) and INCDNT (Incident).
EventDate	j-xsd:date	EVENT	DATE	DATE	A date on which the upload occurred.

<u>Activity</u>		<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about an activity or process that occurs. An activity may encompass a period of time and multiple events.
ActivityID	IDType extends SuperType	INCIDENT ALERT ARREST CHARGE WARRANT	INCIDENT_REPORT _NUM ALERT_ID ARREST_ID CHARGE_ID WARRANT_ID	VARCHAR2 (20) VARCHAR2 (10)	An identifier that uniquely refers to the following documents: Incident Report, Alert, Arrest, charge and warrant.
ActivityOccuranceDate	j-xsd:date	INCIDENT ALERT ARREST CHARGE WARRANT	ACTIVITY_ OCCURANCE_ DATE	DATE	A date of an activity that occurs at a singular point in time or a start date of an activity that occurs over a period of time.
ActivityOfficial. Enforcement	EnforcementOfficialType extends PersonType	ENFORCEMENT_ OFFICIAL	N/A	N/A	An official associated with an activity
ActivityReporting Organization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	The organization primarily associated with the activity.
<u>Alert</u>		<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about an alert used to notify agencies and public systems of an emergency.
AlertEvent	EventType	EVENT	N/A	N/A	The OLLEISN Upload - Alert document.
AlertSubject	SubjectType extends PersonType	PERSON	N/A	N/A	A person who is involved in more than four violent criminal activities, an alert indicator will be set.
AlertAgency	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	The agency that originated the alert.
AlertEnforcementOfficial	EnforcementOfficialType extends PersonType	ENFORCEMENT_ OFFICIAL	N/A	N/A	The enforcement official that originated the alert.
AlertAuditTrail	AuditTrail Type	ALERT	N/A	N/A	An individual or organization can track their record/transaction.

<u>Arrest</u>	<u>ArrestType</u> <u>extends ActivityType</u>	<u>Physical Table Name</u>	<u>Physical Element</u> <u>Name</u>	<u>Physical</u> <u>Element</u> <u>Data Type</u>	
ArrestEvent	EventType	EVENT	N/A	N/A	The OLLEISN Upload - Arrest document.
ArrestSequenceID	IDType extends SuperType	ARREST	SEQUENCE_NUM	VARCHAR2 (10)	A sequential number assigned to the arrest of a subject.
ArrestAgencyRecordID	IDType extends SuperType	ARREST	AGENCY_RECORD_ID	VARCHAR2 (15)	A records management system number of the originating case agency for an arrest. This may be the booking number or the Records Management System number. Sometimes referred to as Originating Case Agency (OCA) number.
ArrestTypeCode	j-nibrs:ArrestTypeCode Type	ARREST	ARREST_TYPE_CODE	VARCHAR2 (5)	A code identifying a type of arrest that occurred.
ArrestSubject	SubjectType extends PersonType	PERSON	N/A	N/A	An individual who is arrested.
ArrestWarrant	SubjectType extends PersonType	WARRANT	N/A	N/A	A court authorized order which commands a peace official to arrest a subject and bring that subject before the court.
ArrestCharge	SubjectType extends PersonType	CHARGE	N/A	N/A	A formal allegation of a violation of a statute and/or ordinance in association with an arrest.
ArrestOfficial	EnforcementOfficialType extends PersonType	ENFORCEMENT_OFFICIAL	N/A	N/A	An official who makes an arrest.
ArrestAgency	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	An agency who originated the arrest.
ArrestSubjectCountCode	j-nibrs:MultipleArrestee SegmentsCodeType	ARREST	MULTIPLE_ARRESTEE_SEQMENTS_CD	VARCHAR2 (10)	A code identifying whether or not to count or score an arrested subject in a system to avoid duplicate counts in the event that the subject may be a part of multiple arrests.
ArrestAuditTrail	AuditTrail Type	ARREST	N/A	N/A	An individual or organization can track their record/transaction.

Charge	ChargeType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	Details about a formal allegation that a specific person has committed a specific offense.
ChargeEvent	EventType	EVENT	N/A	N/A	The OLLEISN upload of the charge document.
ChargeAgencyID	IDType extends SuperType	CHARGE	AGENCY_CHARGE_ID	VARCHAR2 (15)	A unique identifying number assigned to a particular charge by an arresting agency
ChargeSequenceID	IDType extends SuperType	CHARGE	SEQUENCE_ID	VARCHAR2 (15)	A sequentially assigned number for charge tracking purposes (for example, the first charge under the arrest might be assigned Charge Sequence ID 1, the second 2, and so forth).
ChargeTrackingID	IDType extends SuperType	CHARGE	TRACKING_ID	VARCHAR2 (15)	A unique identifying number assigned to an entire set of charges for an arrest. Different numbers may appear in the set if cases have been consolidated.
ChargeCountQuantity	j-xsd:nonNegativeInteger	CHARGE	CHARGE_COUNT_QTY	INTEGER	A number of times a person is charged with committing the same crime.
ChargeOriginator. Organization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	An agency that originally filed a charge.
ChargeOfficial	EnforcementOfficialType extends PersonType	ENFORCEMENT_OFFICIAL	N/A	N/A	A peace official who makes an arrest.
ChargeStatute	StatuteType extends SuperType	STATUTE	N/A	N/A	A unique identifier of a law, rule, or ordinance within a jurisdiction that a person is accused of violating.
ChargeSubject	SubjectType extends PersonType	SUBJECT	N/A	N/A	A person accused of committing a specific offense.
ChargeFelonyIndicator	j-xsd:boolean	CHARGE	FELONY_INDIC	BIT	True if a charge refers to a felony offense; false otherwise. Sometimes referred to as Severity Level.
ChargeSeriousViolent Indicator	j-xsd:boolean	CHARGE	SERIOUS_VIOLENCE_INDIC	BIT	True if a charge filed refers to a serious or violent offense; false otherwise.

ChargeNCICCode	j-ncic:OFFType	CHARGE	NCIC_CD	VARCHAR2 (10)	A code that identifies an offense within the National Crime Information Center (NCIC) system.
ChargeUCRCode	j-ucr:OffenseCodeType	CHARGE	UCR_CD	VARCHAR2 (10)	A code that identifies an offense within the Uniform Crime Report (UCR) system.
ChargeLocalCode	NonStandardCodeType extends SuperType	CHARGE	LOCAL_CD	VARCHAR2 (15)	A local statute or ordinance that identifies an offense.
ChargeAuditTrail	AuditTrail Type	CHARGE	N/A	N/A	An individual or organization can track their record/transaction.
<u>Incident</u>	<u>IncidentType extends ActivityType</u>	Details about a criminal or non-criminal activity that occurred.			
IncidentEvent	EventType	EVENT	N/A	N/A	The event is the OLLEISN upload of the incident document.
IncidentStolenVehicle Quantity	QuantityType extends NumericType	INCIDENT	STOLEN_VEHICLE_QTY	NUMBER (2)	
IncidentAuditTrail	AuditTrail Type	INCIDENT	N/A	N/A	An individual or organization can track their record/transaction.
<u>IncidentCategory</u>	<u>IncidentCategoryType extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details that describe a general category or classification of an incident.
IncidentCriminalIndicator	j-xsd:boolean	INCIDENT	CRIMINAL_INDIC	BIT	True if an incident that occurred is criminal; false if an incident is non-criminal.
IncidentCategoryType Code	j-nibrs:CriminalActivity TypeCodeType	INCIDENT	CATEGORY_TYPE_CD	VARCHAR2 (10)	A code that identifies a type of incident that occurred.
IncidentLevelCode	j-mn_off:OffenseLevel CodeType	INCIDENT	LEVEL_CD	VARCHAR2 (5)	A code identifying a level of an incident, e.g., felony.
<u>IncidentResponse</u>	<u>IncidentResponseType extends ActivityType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about a response to an incident by an official unit.
IncidentReportingOfficial	EnforcementOfficialType extends PersonType	ENFORCEMENT_OFFICIAL	N/A	N/A	A peace official that submitted an incident report in an incident.

IncidentResponse Organization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	An organization or agency that responded to an incident.
IncidentArrestMade Indicator	j-xsd:boolean	INCIDENT	ARREST_MADE_ INDIC	BIT	
Statute	StatuteType extends SuperType	Physical Table Name	Physical Element Name	Physical Element DataType	Details about a unique identifier of a law, rule, or ordinance within a jurisdiction.
StatuteCodeID	IDType extends SuperType	STATUTE	STATUTE_CD_ID	VARCHAR2 (10)	An identifier of a set of laws for a particular jurisdiction. Sometimes referred to as a code book, legal code, native state code, or law.
StatuteOffenseCode.	j-ucr:OffenseCodeType	STATUTE	OFFENSE_CD	VARCHAR2 (10)	A code that identifies a criminal offense within a code book. Sometimes referred to as offense code, ordinance number.
StatuteTypeCode	j- mn_off:StatuteTypeCode Type	STATUTE	TYPE_CD	VARCHAR2 (10)	A code identifying a type of statute, e.g., Criminal, Procedure.
StatuteLevelText	TextType	STATUTE	OFFENSE_LEVEL	VARCHAR2 (20)	A level of crime a statute applies to, e.g., Misdemeanor, Gross Misdemeanor, Felony.
Warrant	WarrantType extends CourtOrderType	Physical Table Name	Physical Element Name	Physical Element DataType	An authorization for an enforcement official to perform a specified action such as arresting a person or searching a residence.
WarrantOriginator Organization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	
WarrantEnforcement Official	EnforcementOfficialType extends PersonType	ENFORCEMENT_ OFFICIAL	N/A	N/A	
WarrantSubject	SubjectType extends PersonType	PERSON	N/A	N/A	

DATABASE PHYSICAL TABLE - ELEMENTS					DEFINITIONS
<u>Aircraft</u>	AirCraftType extends VehicleBasicsType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about a mode of transportation capable of flying in the air.
AircraftTailID	IDType extends SuperType	VEHICLE_BOAT_AIRCRAFT	AIRCRAFT_TAFT_ID	VARCHAR2 (20)	An identifier of an aircraft. Sometimes referred to as a tail number.
AircraftMakeCode	j-ncic:VMAType	VEHICLE_BOAT_AIRCRAFT	AIRCRAFT_MAKE_CD	VARCHAR2 (10)	A code identifying a manufacturer of an aircraft.
AircraftModelCode	j-ncic:VMOType	VEHICLE_BOAT_AIRCRAFT	AIRCRAFT_MODEL_CD	VARCHAR2 (10)	A code identifying a specific design or type of vehicle made by a manufacturer.
AircraftYearDate	j-xsd:gYear	VEHICLE_BOAT_AIRCRAFT	AIRCRAFT_YEAR	NUMBER (4)	A year which is assigned to a vehicle by the manufacturer.
AircraftStyleCode	j-ncic:VSTType	VEHICLE_BOAT_AIRCRAFT	AIRCRAFT_STYLE_CD	VARCHAR2 (10)	A code identifying a style of a vehicle.
AircraftAirportID	IDType extends SuperType	VEHICLE_BOAT_AIRCRAFT	AIRPORT_CD	VARCHAR2 (20)	An identifying number of an airport at which an aircraft lands or is kept. Sometimes referred to as an airport code.
<u>Boat</u>	BoatType extends VehicleBasicsType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about a vessel for transport by water, constructed to provide buoyancy by excluding water and shaped to give stability and permit propulsion.
BoatRegistrationID	IDType extends SuperType	VEHICLE_BOAT_AIRCRAFT	BOAT_REGISTRATION_ID	VARCHAR2 (20)	An identifier assigned to a vessel by the coast guard or another vessel licensing organization.
BoatMakeCode	j-ncic:BMAType	VEHICLE_BOAT_AIRCRAFT	BOAT_MAKE_CD	VARCHAR2 (10)	A code identifying the manufacturer of a vessel.
BoatTypeCode	j-ncic:BTYType	VEHICLE_BOAT_AIRCRAFT	BOAT_TYPE_CD	VARCHAR2 (10)	A code identifying the type of a vessel.
BoatColorCode	j-ncic:BCOType	VEHICLE_BOAT_AIRCRAFT	BOAT_COLOR_CD	VARCHAR2 (10)	A code identifying the color of a vessel.
BoatHullID	IDType extends SuperType	VEHICLE_BOAT_AIRCRAFT	BOAT_HULL_ID	VARCHAR2 (10)	An identifier found on a vessel's hull.

BoatHullSerialID	IDType extends SuperType	VEHICLE_BOAT_ AIRCRAFT	BOAT_HULL_ SERIAL_NUM	VARCHAR2 (20)	An identifying number inscribed on or attached to a part, collection of parts, or complete unit by the manufacturer.
BoatHullMaterialCode	j-ncic:HULType	VEHICLE_BOAT_ AIRCRAFT	BOAT_HULL_ MATERIAL_CD	VARCHAR2 (10)	A code identifying a primary construction material of a vessel's hull.
BoatHullShapeCode	j-ncic:HSPTType	VEHICLE_BOAT_ AIRCRAFT	BOAT_HULL_ SHAPE_CD	VARCHAR2 (10)	A code identifying a shape and configuration of a hull on a vessel.
BoatTrailerMakeName	TextType	VEHICLE_BOAT_ AIRCRAFT	TRAILER_MAKE_ NAME	VARCHAR2 (20)	A make of a boat trailer.
BoatTrailerMakeCode	j-ncic:BTMAType	VEHICLE_BOAT_ AIRCRAFT	TRAILER_MAKE_CD	VARCHAR2 (10)	A code identifying a make of a boat trailer.
<u>Property</u>	PropertyType extends SuperType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	A tangible or intangible item that can be owned or used.
PropertyTypeCode	j-ncic:TYPAType	PROPERTY	TYPE	VARCHAR2 (10)	A code that identifies a type of property.
PropertyConditionText	TextType	PROPERTY	CONDITION	VARCHAR2 (30)	A state or appearance of a property item, e.g., new, used, damaged.
PropertyOwner. Organization	OrganizationType extends SuperType	ORGANIZATION	N/A	N/A	Details about a person or organization which own a property item.
PropertyOwner.Person	PersonType extends SuperType	PERSON	N/A	N/A	Details about a person or organization which own a property item.
PropertyStatus	StatusType extends SuperType	PROPERTY	STATUS	VARCHAR2 (20)	A status of a property item. Describes if the property is being held, is stolen, missing, recovered, damaged, no change.
PropertyAuditTrail	AuditTrail Type	PROPERTY	N/A	N/A	An individual or organization can track their record/transaction.
<u>PropertyDisposition</u>	PropertyDisposition Type extends ActivityType	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about what has happened to a property item.

PropertyDispositionCode	j-nibrs:PropertyLossCode Type	PROPERTY	DISPOSITION_CD	VARCHAR2 (10)	A code that identifies what happened to a property item, e.g., towed, released, seized, unrecoverable, missing, stolen.
<u>Vehicle</u>	<u>VehicleType</u> <u>extends</u> <u>VehicleBasicsType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about a motor-driven conveyance designed to carry its operator, passengers, and cargo, including trailers, and excepting boats.
VehicleID	<u>DrivingJurisdiction AuthorityIDType</u> <u>extends IDType</u>	VEHICLE_BOAT_AIRCRAFT	VEHICLE_ID_NUM	VARCHAR2 (10)	A unique combination of alphanumeric characters that identifies a specific vehicle. A vehicle identification number is normally imprinted by the manufacturer and attached to the vehicle in specific locations, but is occasionally assigned by titling or registration agencies. Sometimes referred to as a VIN, VIN number.
VehicleLicensePlateID	<u>IDType</u> <u>extends SuperType</u>	VEHICLE_BOAT_AIRCRAFT	VEHICLE_LICENSE_PLATE_ID	VARCHAR2 (20)	License plate associated with a vehicle
VehicleMakeCode	j-ncic:VMAType	VEHICLE_BOAT_AIRCRAFT	VEHICLE_MAKE_CD	VARCHAR2 (10)	A code identifying the manufacturer of a vehicle.
VehicleModelCode	j-ncic:VMOType	VEHICLE_BOAT_AIRCRAFT	VEHICLE_MODEL_CD	VARCHAR2 (10)	A code identifying the specific design or type of vehicle made by a manufacturer. Sometimes referred to as the series model.
VehicleModelYearDate	j-xsd:gYear	VEHICLE_BOAT_AIRCRAFT	VEHICLE_YEAR	NUMBER (4)	A year which is assigned to a vehicle by the manufacturer.
VehicleModelCodeText	<u>TextType</u>	VEHICLE_BOAT_AIRCRAFT	VEHICLE_MODEL_CD	VARCHAR2 (10)	A code denoting a family of vehicles within a vehicle make which has a degree of similarity in construction, such as body, chassis, etc. The field does not necessarily contain a standard code; it may contain a value provided by the originator (the manufacturer) of the field.
VehicleStyleCode	j-ncic:VSTType	VEHICLE_BOAT_AIRCRAFT	VEHICLE_STYLE_CD	VARCHAR2 (10)	A code identifying the style of a vehicle.

VehicleColorPrimary Code	j-ncic:VCOType	VEHICLE_BOAT_AIRCRAFT	VEHICLE_COLOR_PRIMARY_CD	VARCHAR2 (10)	A code identifying a single, upper-most, front-most, or majority color of a vehicle.
VehicleColorSecondary Code	j-ncic:VCOType	VEHICLE_BOAT_AIRCRAFT	VEHICLE_ICOLOR_SECONDARY_CD	VARCHAR2 (10)	A code identifying the lower-most or rear-most color of a two-tone vehicle or the lesser color of a multi-colored vehicle.
<u>VehicleBasics</u>	<u>VehicleBasicsType extends PropertyType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	Details about a vehicle, boat, aircraft, or other object used to provide a physical mode of transportation
VehicleRegistration	<u>VehicleRegistrationType extends PropertyRegistrationType</u>	N/A	N/A	N/A	Details about a registration of a vehicle.
VehicleWantedIndicator	j-xsd:boolean	VEHICLE_BOAT_AIRCRAFT	VEHICLE_WANTED_INDIC	BIT	True if a vehicle is being searched for by law enforcement; false otherwise.

DATABASE PHYSICAL TABLE - ELEMENTS					DEFINITIONS
<u>AuditTrail</u>	<u>AuditTrailType extends SuperType</u>	<u>Physical Table Name</u>	<u>Physical Element Name</u>	<u>Physical Element DataType</u>	
AgencyUserRecordOwner	ACTIVITY_TYPE ARREST_TYPE CHARGE_TYPE CONTACT_PHONE_EMAIL INCIDENT_TYPE LOCATION_TYPE ORGANIZATION_TYPE PERSON_TYPE PROPERTY_TYPE	ALERTY_TYPE ARREST_TYPE CHARGE_TYPE CONTACT_PHONE_EMAIL INCIDENT_TYPE LOCATION_TYPE ORGANIZATION_TYPE PERSON_TYPE PROPERTY_TYPE WARRANT_TYPE	AGENCY_USER_OWNER	VARCHAR2 (30)	The agency-owner who owns the record
AgencyUserCreateUdpate DeleteDate			AGENCY_USER_CRT_UPDT_DEL_DATE	DATE	The agency-owner who created, update or deleted a record
VendorTransactionKey			VENDOR_TRANSACTION_KEY	VARCHAR2 (20)	A key a vendor can utilize to track their records.

<u>AgeMeasure</u>	<u>AgeMeasureType</u> <u>extends MeasureType</u>	A representation of an age.
@ageUnitCode	AgeUnitCodeType	A code that identifies the unit of measure of the age value.
<u>IDObject</u>	<u>IDType</u> <u>base xsd:string</u> <u>extends SuperType</u>	Information that identifies an entity.
ID	TextType	A value that identifies an entity within the identifier domain.
IDTypeText	TextType	A type of identifier assigned.
IDTypeDescriptionText	TextType	A description of a type of identifier.
IDTypeCodeText	TextType	A textual code representing the type of identifier assigned.
IDTypeCodeSourceText	TextType	A source of the identifiers type code.
IDTypeCodeVersionText	TextType	A source version of the identifiers type code.
IDStatus	StatusType extends SuperType	A condition or state of an identifier, e.g., valid, expired.
IDEffectiveDate	j-xsd:date	A date an identifier becomes effective. This may or may not be the issue date.
IDExpirationDate	j-xsd:date	A date an identifier is no longer valid.
IDSourceText	TextType	The locale or organization from which an identification originates.
<u>Measure</u>	<u>MeasureType</u> <u>base xsd:decimal</u> <u>extends SuperType</u>	A representation of a measurement.
@measureUnitText	xsd:string	A unit that qualifies the measurement value.
@measureDate	xsd:date	A date a measurement was made.
@measureTime	xsd:time	A time a measurement was made.
@measurerName	xsd:string	A name of a person or organization that made a measurement.
@measurerID	xsd:string	An identifier of a person or organization that made a measurement.
@measurementTypeText	xsd:string	A method used to make a measurement.

@measurementEstimatedIndicator	xsd:boolean	True if a measurement has been estimated or guessed; false otherwise.
<u>RangeMeasure</u>	<u>RangeMeasureType</u> <u>extends SuperType</u>	A minimum - maximum range between two measured values.
RangeMinimumMeasure	<u>MeasureType</u> <u>extends SuperType</u>	A minimum measure value on a range measure.
RangeMaximumMeasure	<u>MeasureType</u> <u>extends SuperType</u>	A maximum measure value on a range measure.
<u>Status</u>	<u>StatusType</u> <u>base xsd:string</u> <u>extends SuperType</u>	A set of details about the condition or status of a person, activity, or object.
StatusText	<u>TextType</u>	A condition or state of something or someone.
StatusDate	j-xsd:date	A date a status was set, effective, or reported.
StatusTime	j-xsd:time	A time a status was set, effective, or reported.
StatusIssuerText	<u>TextType</u>	A name or code of a person or organization which assigns a status.
StatusDescriptionText	<u>TextType</u>	A description of a condition or state of something or someone.
StatusIssuerID	<u>IDType</u> <u>extends SuperType</u>	An identifier of a person or organization which assigns a status.
<u>SuperObject</u>	<u>SuperType</u>	The root object in the inheritance hierarchy.
@languageText	xsd:string	The language in which the data content is recorded.
@distributionText	xsd:string	The allowable recipients of this contents. Dissemination statement or instructions.
@sensitivityText	xsd:string	Information security classification level (e.g., FOUO = For Official Use Only)
@sourceText	xsd:string	The name or id of an information resource from which the content came.
@reportingPersonText	xsd:string	Identifies a person (name or id) who provided the information.
@reportingPersonRoleText	xsd:string	Indicates the type, responsibility, or role of person who provided the information.
@reportingOrganizationText	xsd:string	Indicates an organization (name or id) that provided the information (may be associated with the person above).

@reportedDate	xsd:date	The date information was observed, measured, identified or became known.
@effectiveDate	xsd:date	The date that information becomes active or accurate.
@expirationDate	xsd:date	The date information becomes inactive or is no longer valid.
@sourceIDText	xsd:string	A number or string set by a data provider so that information that is sent can be retraced back to its source, e.g., a combination of the data source name, table name, and record ID. This ID is meaningful only to the data provider.
@criminalInformationIndicator	xsd:boolean	True if the information specified is classified as criminal information; false if it is not classified as criminal information.
@intelligenceInformationIndicator	xsd:boolean	True if the information specified is intelligence information; false otherwise.
<u>Text</u>	<u>TextType</u>	A representation of a string value.
@languageCode	iso_639-2:LanguageCodeType	The language in which the strings content is recorded.
<u>TimeMeasure</u>	<u>TimeMeasureType</u> <u>extends MeasureType</u>	A representation of the measurement of an amount of time.
@timeUnitCode	unece:TimeType	A code that identifies the unit of measure of the time value.
<u>WeightMeasure</u>	<u>WeightMeasureType</u> <u>extends MeasureType</u>	A representation of the measurement of a weight.
@weightUnitCode	unece:MassType	A code that identifies the unit of measure of the weight value.

APPENDIX C
LOCAL DATA ELEMENTS

APPENDIX D
STEERING COMMITTEE LISTING

OHIO ASSOCIATION OF CHIEFS OF POLICE
LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM
LOCAL LAW ENFORCEMENT INFORMATION SHARING AND
COMMUNICATIONS NETWORK
STEERING COMMITTEE LISTING

2004

Chief Gary Vest, Chair

Powell PD
260 Village Park Dr.
Powell, OH 43065
Phone: 614-885-5005
Fax: 614-885-5594
E-mail: *chiefvest@rrohio.com*

Darryl L. Anderson
MARCS Program Manager
2323 W. Fifth Ave, Suite 150
Columbus, OH 43240
Phone: 614-466-2257
Fax: 614-995-0067
E-mail: *darryl.anderson@das.state.oh.us*

Chief Michael J. Clancey
Westerville PD
29 S. State Street
Westerville, OH 43081
Phone: 614-901-6466
Fax: 614-901-6465
E-mail: *mclancey@westerville.org*

Major Stephen Friday
Ohio State Highway Patrol
1970 West Broad Street
Columbus, OH 43223
Phone: 614-466-3554
Fax: 614-466-8243
E-mail: *sfriday@dps.state.oh.us*

Chief Matthew E. Fruchey, CLEE
Glendale PD
301 E. Sharon Road
Glendale, OH 45246
Phone: 513-771-7645
Fax: 513-771-7882
E-mail: *mfruchey@glendaleohio.org*

Captain Michael Goodwin
New Philadelphia PD
122 Second St. SE
New Philadelphia, OH 44663
Phone: 330-343-4487
Fax: 330-343-4488
E-mail: *nppd@tusco.net*

Chief Charles Goss
Strongsville PD
18688 Royalton Road
Strongsville, OH 44136
Phone: 440-238-1048
Fax: 440-238-1642
E-mail: *cgoss@strongsvillepolice.com*

Chief Gerald O. Herman
Northwood PD
6000 Wales Road
Northwood, OH 43619-1480
Phone: 419-691-5053
Fax: 419-693-3515
E-mail: *600@northwoodpolice.com*

Director Karen Huey
Ohio Criminal Justice Services
140 East Town Street, 14th Floor
Columbus, OH 43215
Phone: 614-466-7782
Fax: 614-466-5061
E-mail: *huey@ocjs.ohio.gov*

Sheriff Rocky Nelson
Union County Sheriff's Office
221 W. 5th Street
Marysville, OH 43040
Phone: 937-645-4100
Fax: 937-645-4170
E-mail: *rnelson@co.union.oh.us*

Captain Thomas Pyle
Athens PD
11 North College Street
Athens, OH 45701
Phone: 740-592-3315
Fax: 740-592-3358
E-mail: *tpyle@ci.athens.oh.us*

Deputy Superintendent Steve Raubenolt
Ohio Law Enforcement Gateway
150 E. Gay Street, 16th Floor
Columbus, OH 43215
Phone: 614-387-7622
Fax: 614-466-6727
E-mail: *SRAubenolt@ag.state.oh.us*

Chief Wayne Willcox, CLEE
Piqua PD
100 N. Wayne Street
Piqua, OH 45356
Phone: 937-778-2023
Fax: 937-778-5145
E-mail: *wwillcox@piquaoh.org*

Director Patrick Wright
Northwest Ohio Reg. Information System
Criminal Justice Coordinating Council
One Government Center, Suite 1720
Toledo, OH 43604
Phone: 419-213-3838
E-mail: *pat.wright@NORIS.org*

Dr. Todd Wurschmidt
Executive Director
Ohio Association of Chiefs of Police
6277 Riverside Drive, Suite 2N
Dublin, OH 43017
Phone: 614-761-0330
Fax: 614-718-3216
E-mail: *todd.wurschmidt@oacp.org*

Dr. Ted Oakley, Program Director
Ohio Association of Chiefs of Police
6277 Riverside Drive, Suite 2N
Dublin, OH 43017
Phone: 614-761-0330
Fax: 614-761-9509
E-mail: *ted.oakley@oacp.org*

APPENDIX E
GLOSSARY

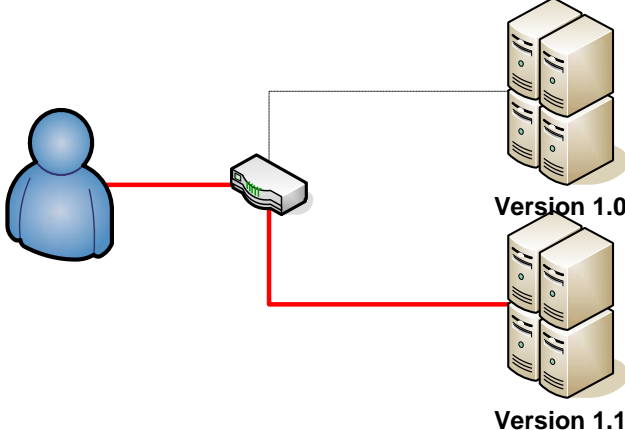
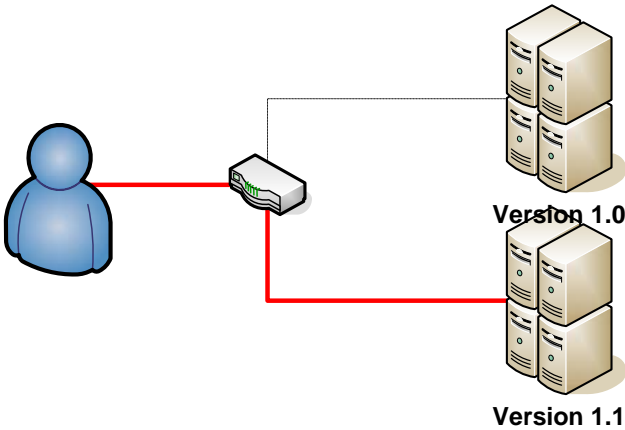
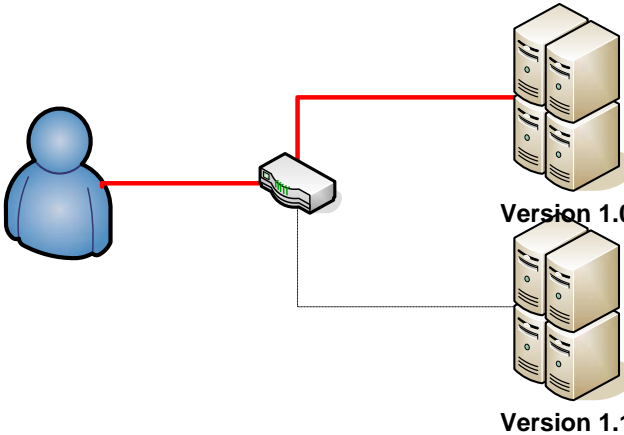
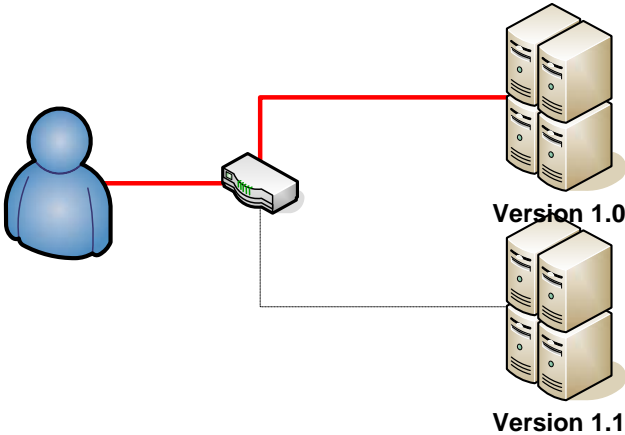
GLOSSARY

Acronym	Definition
ASP	Active Server Page
BSSA	Buckeye State Sheriffs' Association
CAD	computer-aided dispatch
DAS	Department of Administrative Services
DBA	database administrator
DOJ	Department of Justice
FTE	full-time employee
GJXDM	Global Justice XML Data Model
HP	Hewlett-Packard
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MARCS	Mobile Area Radio Communication System
MDT	mobile data terminal
OACP	Ohio Association of Chiefs of Police
OAG	Ohio Attorney General
OCJS	Office of Criminal Justice Services
ODPS	Ohio Department of Public Safety
OHLEG	Ohio Law Enforcement Gateway
OIBRS	Ohio Incident-Based Reporting System
OLLEISN	Ohio Local Law Enforcement Information-Sharing Network
OPOTA	Ohio Peace Officer Training Academy
OSHP	Ohio State Highway Patrol
RMS	records management system
SAN	Storage Area Network
SQL	Structured Query Language
TB	terabyte
TCO	total cost of ownership
UCR	Uniform Crime Reporting
VPN	virtual private network
XML	eXtensible Markup Language

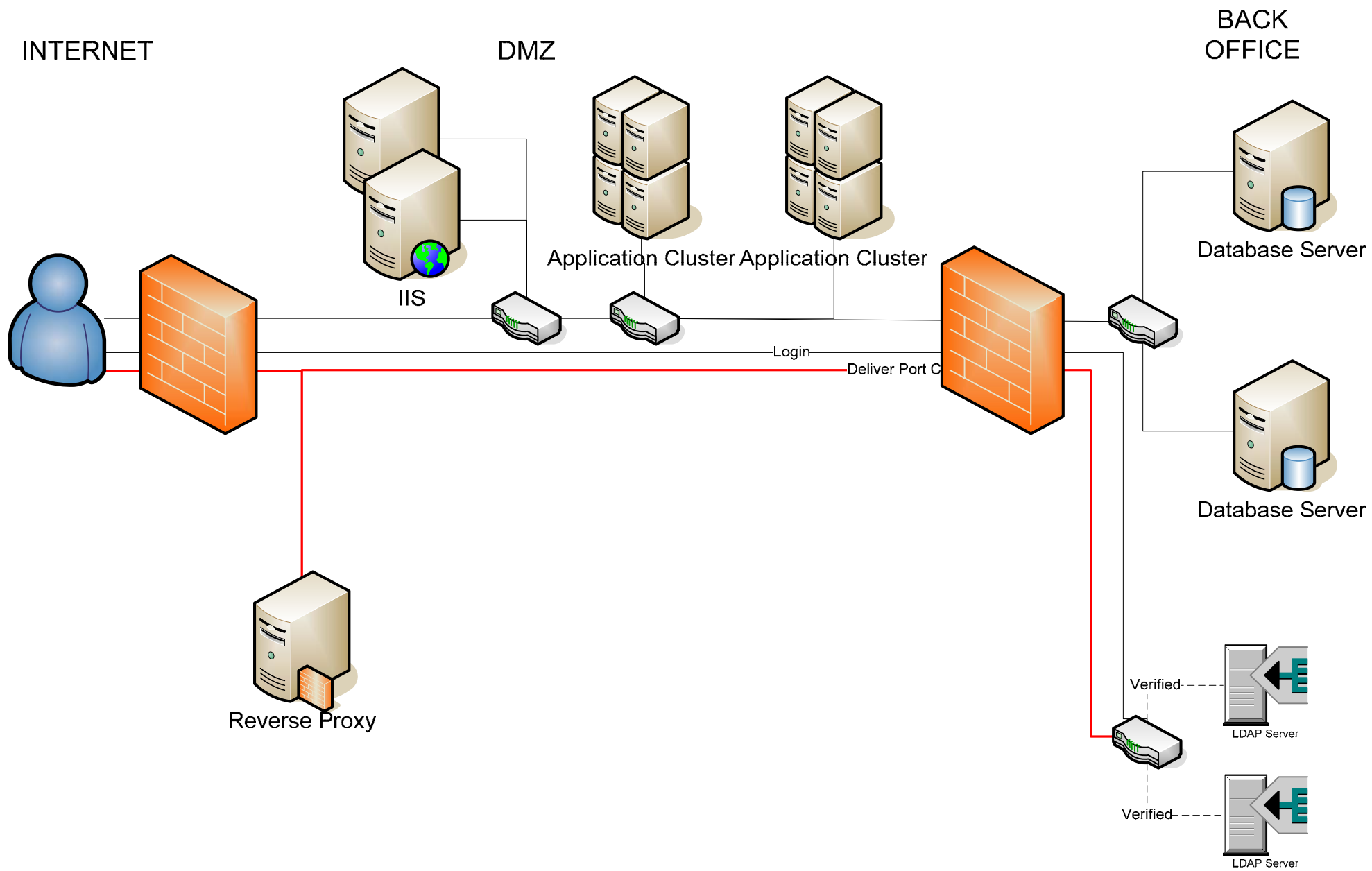
APPENDIX F
DIAGRAM OF STAGING / RELEASE PROCEDURES

Columbus, Ohio Data Center

London, Ohio Data Center

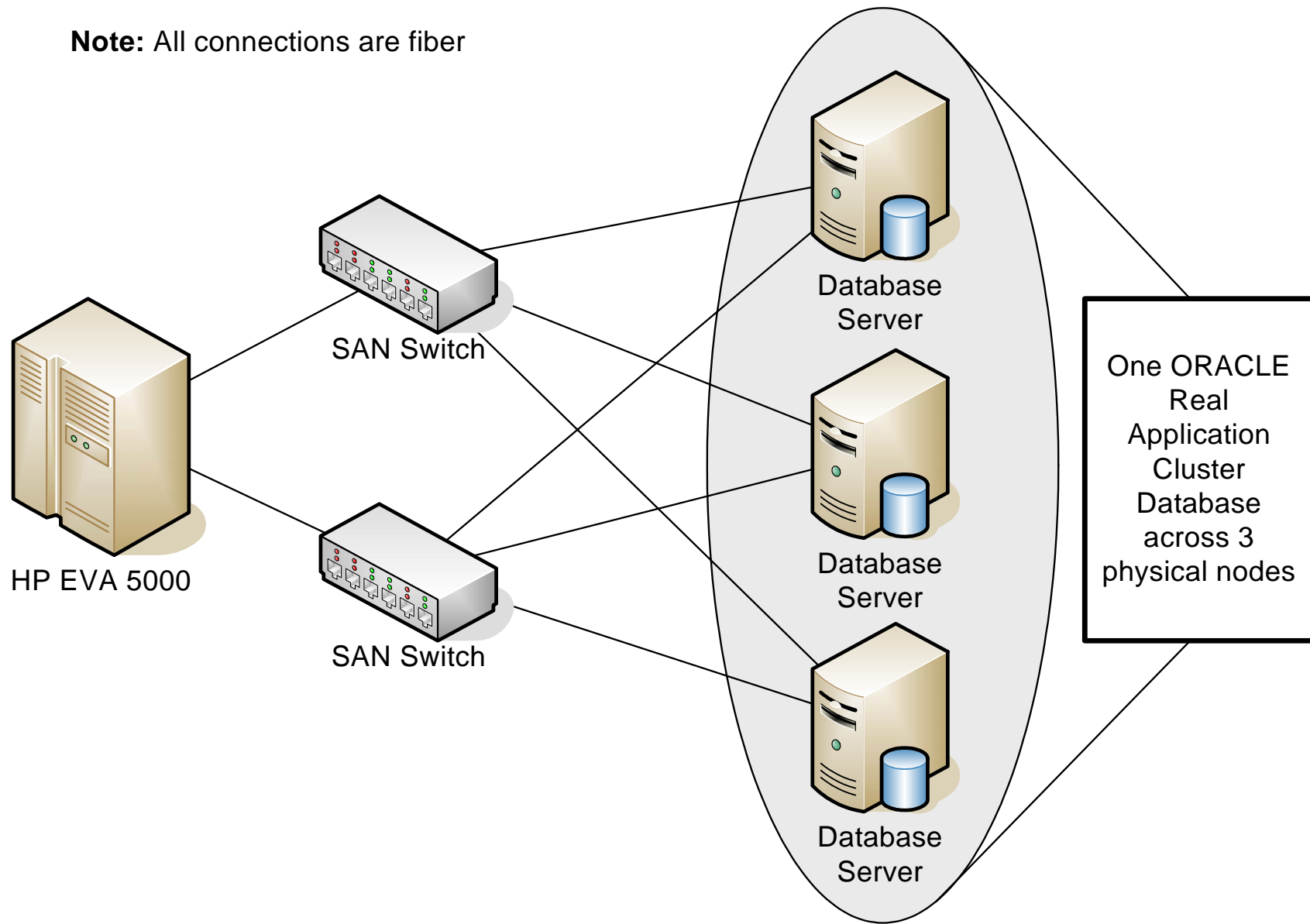


APPENDIX G
DIAGRAM OF OHLEG NETWORK ARCHITECTURE



APPENDIX H
DIAGRAM OF SAN AND ORACLE DATABASE ARCHITECTURE

Note: All connections are fiber



APPENDIX I

OHLEG SECURITY - USER ADMINISTRATION

OHLEG Security Model

All communication with the OHLEG takes place via a browser and three forms of authentication have been standardized. They are the username, password and ORI number. These three credentials are needed to access any and all applications that are available in the OHLEG as a link, once authenticated.

The Username is comprised of the initial of first name concatenated with the last name and the last five digits of the user's Social Security Number. Passwords must be six characters in length. Originating Agency Identifier (ORI) means a unique, nine-character identifier assigned by the Law Enforcement Automated Data System (LEADS) and the National Crime Information Center (NCIC) to electronically address each agency and terminals within the agency. The ORI number is required for any person requesting access to the OHLEG.

Currently there are over 30,000 peace officers defined in OHLEG as possible users. This number will continue to grow as we introduce Ohio Highway State Patrol officers, state prosecutors and the Department of Rehabilitation and Corrections personnel. OHLEG was designed with this in mind and is scalable to handle the increase in the number of users.

The idea incorporated in the OHLEG is one of "one stop shopping". Once authenticated a single sign on process controls future authentications. Therefore, the user will only have to authenticate once instead of multiple times for multiple applications. Novell products eDirectory, iCHAIN and DirXML are utilized to accomplish this security model and scalability.

Novell® eDirectory® is scalable to accommodate over one million users. For over a decade Novell eDirectory has defined and reinvented the role of a directory service. More than just an LDAP data store, eDirectory® is the identity foundation that links your users and their access rights with corporate resources, devices and security policies. Among directory services, eDirectory® is uniquely capable of meeting the demands of large-scale, high-end directory deployments. It offers the compatibility, security, reliability, scalability and manageability required for internal and Internet deployments supporting millions of identities.¹

Novell® iChain® is an integrated security solution that offers secure authentication and access to portals, Web-based content and Citrix* Thin Client services. It includes identity-based Web security services and enables authorized users—including employees, customers and partners—to securely authenticate from anywhere, at any time. Novell® iChain® simplifies administration, secures irreplaceable data and accelerates your access to information and overall eBusiness integration.² ICHAIN utilizes reverse proxy, control session management and single sign on at the AGO.

Novell Nsure Identity Manager 2—formerly DirXML®—helps you securely manage the access needs of your ever-changing user community. With Nsure Identity Manager, you can manage the full user lifecycle—deliver first-day access to essential resources, synchronize multiple passwords into a single login, modify or revoke access rights instantly and even support compliance with government regulations. Nsure Identity Manager also provides self-service features that enable users to maintain their own passwords and profile information. With these capabilities you will realize tangible business benefits: streamlined administration, increased security, reduced costs and a swift return on investment (ROI).³ The AGO utilizes DirXML as a federation to tie LDAP database users and applications together.

¹ <http://www.novell.com/products/edirectory/quicklook.html>

² <http://www.novell.com/products/ichain/quicklook.html>

³ <http://www.novell.com/products/nsureidentitymanager/quicklook.html>

Current applications available through the OHLEG are FinCrime (Financial Crime alert and database system), eSORN (electronic Sex Offender Registration and Notification) and CCW (Carry Concealed Weapons).

Our current security model is a multi-tiered security model. Individuals that are able to create the users are not the same individuals that are able to grant the users access to applications. Therefore, no single individual is able to create a username and grant inappropriate rights to applications.

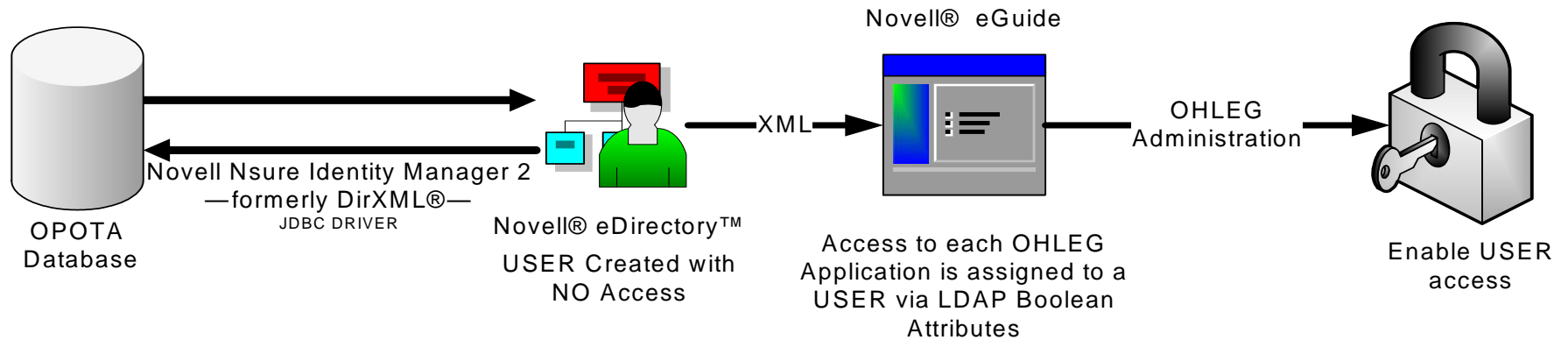
OHLEG Security - Administrative Policy

Ohio Revised Code Section 109.761 requires any agency or department to report to the Commission any peace officer appointments or terminations within 10 days of their occurrence. The law became effective on February 20, 2002. The law also requires the reporting of an annual roster of persons appointed to function as peace officer within any agency/entity. The Director of the Ohio Peace Officer Training Commission (OPOTC) sets the reporting date and the annual roster is usually a computer-generated report of all current records in the Peace Officer Listing, Academy Registration and Information System (POLARIS). The report is sent to the chief or sheriff and they make any corrections and send the appropriate documentation for the changes back to the Commission.

New appointments, appointment status changes, corrections (including name changes), and terminations must be reported via the Form SF400adm - Notice of Peace Officer Appointment/Termination. The forms are received by OPOTC and a certification officer evaluates the data contained within. If a peace officer is evaluated and deemed current on all training and certifications then the information is entered into POLARIS indicating the officer has been verified and is in good standing. If a peace officer is not current, information is entered into POLARIS indicating any training or additional information expected back from the officer.

In order to have an OHLEG login, the following information needs to be entered into POLARIS. We must have a SSN, first name, last name, date of birth, the agency with whom they are currently employed, their starting date with that agency and their status (i.e., part time, full time, etc). Once an officer is terminated or resigns from the agency it is required that the agency notify the OPOTC of this change and an ending date is placed on their employment record. This event will trigger the deactivation of the peace officer's OHLEG account.

OHLEG USER Administration



EXAMPLE

John Doe will have access to OHLEG/SE and ONLY OHLEG/SE.

Name: John Doe	
eSORN Access:	FALSE
OHLEG/SE Access:	FALSE
FinCrime Access:	FALSE

OHLEG
Administration

Name: John Doe	
eSORN Access:	FALSE
OHLEG/SE Access:	TRUE
FinCrime Access:	FALSE