



## IV. OJIN ARCHITECTURE

This section presents the OJIN Architecture Model. It defines an architecture that enables the exchange and sharing of criminal justice-related information among authorized agencies. It has been designed to transition from Ohio's current criminal justice data exchange model to an Internet-based paradigm that minimizes the impact on participating agencies while providing a secure environment that protects information and system accessed via OJIN from unauthorized access.

This section identifies the technologies, standards, products and configurations for the OJIN domain architectures. These domains include the centralized OJIN environment as well as the participating, both contributing and non-contributing, agencies. This section is organized around the definition of each domain architecture as follows:

- ❑ Data Sharing and Transport,
- ❑ OJIN Central Server Design,
- ❑ Agency Server Design,
- ❑ Network Design,
- ❑ OJIN Security,
- ❑ User Device Specifications, and
- ❑ Application Design Architecture.

These design standards conform to the conceptual architecture design principles established in Section III.

### A. DATA SHARING AND TRANSPORT

Section III described three data sharing and transport models supported by the OJIN Architecture – Centralized, Distributed, and Hybrid. Contributing agencies may select which model they will implement. Therefore, the OJIN Architecture must support any combination of data sharing models and must be sufficiently flexible to allow agencies to change their model or even use multiple models for different data sources. This section evaluates the various options according to both agency and OJIN perspectives; defines the content of the transaction and associated business rules for updating the OJIN Centralized index as well as agency detailed information located on the OJIN server. Each of these options has been described in Section III.

#### A.1 EVALUATION OF DATA SHARING OPTIONS

*Exhibit IV-1: Summary of Data Sharing Options*, summarizes the level of complexity associated with each option. A down arrow, ↓, represents the lowest level of complexity. Complexity increases according to the symbols —, ↑, with ↑↑ representing the highest complexity level. Complexity is also indicated by the position of the symbol, with the rightmost location indicating the highest level of complexity. *Exhibit IV-2: Evaluation of Data Sharing Options*, explains the complexities of each Data Sharing Option and compares / evaluates the applicability of the three OJIN data sharing options.



**Exhibit IV-1  
SUMMARY OF DATA SHARING OPTIONS**

	Centralized Option	Hybrid Option	Distributed Option
Data Currency	↓	↑	↑
Data Synchronization	↑	↓	↑
Availability	↓	↑	↑
Agency Implementation Effort	↓	↑	↑↑
Agency Capacity	—	↑	↑↑
OJIN Capacity	↑	—	—
Agency System Consistency	↓	↑	↑
Operational Support	↓	—	↑

*Exhibit IV-2: Evaluation of Data Sharing Options*, explains the complexities of each Data Sharing Option and compares / evaluates the applicability of the three OJIN data sharing options.



**Exhibit IV-2 (Page 1 of 2)**  
**EVALUATION OF DATA SHARING OPTIONS**

	<b>Centralized Option</b>	<b>Hybrid Option</b>	<b>Distributed Option</b>
Data Currency	Currency of Detailed Data is dependent the Contributing Agency's Update Schedule.	There is no delay between the update of Detailed Data in the Contributing Agency's application and the availability of the updated data to OJIN users.	There is no delay between the update of Detailed Data in the Contributing Agency's application and the availability of the updated data to OJIN users.
Data Synchronization	Index and Detailed Data is updated concurrently.	There will typically be a delay between the updates to the Contributing Agency's detailed data and the corresponding update to the Centralized Index information. It is possible to have an index record without corresponding detailed data.	Index and Detailed Data is updated concurrently.
Availability	Access to index and detailed data requires availability of the OJIN environment only.	Access to index and detailed data requires availability of both the OJIN and Contributing Agency environments.	Access to index and detailed data requires availability of both the OJIN and Contributing Agency environments.
Agency Implementation Effort	Requires the lowest level of agency effort to implement. Contributing Agency generates only an extract file.	Contributing Agency must: <input type="checkbox"/> create OJIN Index Update transactions as a result of updates to the relevant agency database, <input type="checkbox"/> forward data to OJIN via standard XML definition or HTML web pages.	Contributing Agency must: <input type="checkbox"/> create a Distributed OJIN Index and synchronize updates to the Index and the Detailed Data, <input type="checkbox"/> forward data to OJIN via standard XML definition or HTML web pages.
Capacity	Does not require additional technical resource infrastructure capacity from the Contributing Agency. Requires a higher OJIN centralized database capacity.	Requires that the Contributing Agency system has sufficient capacity to handle queries against the relevant agency database(s).	Requires the Contributing Agency to have sufficient: <input type="checkbox"/> performance capacity to handle queries against the OJIN Index and the relevant agency database(s), and <input type="checkbox"/> database capacity for the OJIN Index. Increases overall traffic on the LEADS network. Does not increase centralized OJIN technical capacities.



**Exhibit IV-2 (Page 2 of 2)  
EVALUATION OF DATA SHARING OPTIONS**

	<b>Centralized Option</b>	<b>Hybrid Option</b>	<b>Distributed Option</b>
Agency System Compatibility	Easiest option to implement for Contributing Agency Legacy systems with non-relational database systems.	Suited to Contributing Agency web-based client-server agency systems that utilize an RDMBS.	Suited to Contributing Agency web-based client-server agency systems that utilize an RDMBS.
Operational Support	Requires the least amount of Contributing Agency’s resources.	Requires a medium level of the Contributing Agency’s resources.	Requires the highest level of Contributing Agency’s resources.

**A.2 DATA MAINTENANCE TRANSACTIONS**

This section describes the content of the OJIN data maintenance transactions and associated business rules for updating the OJIN Centralized Index as well as OJIN Detailed Data located on the OJIN server.

**A.2.1 Index Update Transaction**

One component of the OJIN Information Architecture is an index of subject information that can be searched via the Subject Query transaction to identify and retrieve information concerning a particular individual involved in the criminal justice process. Section II presented a logical data model for the OJIN index information. The OJIN index can either be centralized or distributed, that is, its location is either on the OJIN database server or on the contributing agency’s database server. Regardless of the location of the OJIN index, it must conform to the logical data model defined in Section II.

For an OJIN Centralized Index, the contributing agency is responsible for regularly updating the information contained on the index. This update must be synchronized with the corresponding update to the detailed information. Contributing agencies with a centralized index must generate an OJIN Index Update transaction. Each OJIN Index Update transaction consists of a complete OJIN Index record, it cannot represent an incremental change to an existing OJIN Index record. Part of the OJIN Index record is a “key” that consists of the source agency and a unique identifier. This identifier is created by the agency and must be consistently maintained and associated with the same subject in the agency database. When OJIN receives an OJIN Index Update transaction, the key in the transaction’s OJIN Index record will be compared to records in the existing OJIN Index. Based upon the result of that comparison, OJIN will process the transaction according to the following set of business rules:

- if the key does not exist in the OJIN Index, a new OJIN Index record will be added containing the data from the transaction;



- ❑ if the key exists with an earlier currency date, the OJIN index record will be replaced with the record from the OJIN Index Update transaction;
- ❑ if the key exists and all fields except the key in the transaction are empty, the record will be deleted from the OJIN Index; or
- ❑ if the key exists in the current OJIN Index with a later currency date, the OJIN Index Update transaction will be ignored.

These business rules ensure that the OJIN Index will be updated correctly. They provide the means by which to add, maintain, and delete OJIN Index records. They also ensure that only the contributing agency can maintain OJIN Index records owned by that agency.

## A.2.2 Detail Update Transaction

A second component of the OJIN Information Architecture is a database of detailed information that corresponds to an OJIN Index record. This content and structure of the Detailed Data varies by record type. Record type differentiates among various OJIN data types as identified in Exhibit II-3: Data Access Interest. OJIN will have a standard XML record definition for each OJIN Detailed Record Type. The OJIN Detailed Data can either be centralized or distributed, that is, its location is either on the OJIN database server or on the contributing agency's database server. Centralized OJIN Detailed Data (Codd), detailed data that resides on the OJIN database server, will conform to the standard XML record definition. Distributed OJIN Detailed Data (Dodd) that is retrieved and provided to a user as a result of a Subject Search will be provided by the agency using either the standard XML record definition or HTML pages that are formatted by the agency. The agency database that contains the Dodd may be a standard Database Management System (DBMS), Relational Database Management System (RDBMS), a proprietary database system, or static text files.

For Centralized OJIN Detailed Data, the contributing agency is responsible for regularly updating the information. This update will be synchronized with the corresponding update to the Centralized OJIN Index record, which is the responsibility of OJIN. Contributing agencies with Codd must generate an OJIN Detailed Data Update transaction. OJIN will create or update the OJIN Index automatically. Each OJIN Detailed Data Update transaction consists of a complete Codd record according to the pre-defined XML definition for the record type. The transaction cannot represent an incremental change to an existing Codd record. Part of the Codd record is a "key" that consists of the source agency and a unique identifier. This identifier is created by the agency and must be consistently maintained and associated with the same subject in the agency database. When OJIN receives an OJIN Detailed Data Update transaction, the key in the transaction's record will be compared to records in the existing Centralized OJIN Detailed Data. Based upon the result of that comparison, OJIN will process the transaction according to the following set of business rules:

- ❑ if the key does not exist in the Codd, a new Codd and a new OJIN Index record will be added;



- ❑ if the key exists with an earlier currency date, the CODD record will be replaced with the record from the OJIN Detailed Data Update transaction and the corresponding OJIN Index Record will be synchronized;
- ❑ if the key exists and all fields except the key in the transaction are empty, the CODD record will be deleted from the CODD and OJIN Index; or
- ❑ if the key exists in the CODD with a later currency date, the OJIN Detailed Data Update transaction will be ignored.

These business rules ensure that the Centralized OJIN Detailed Data will be updated correctly. They provide the means by which to add, maintain, and delete CODD records. They also ensure that only the contributing agency can maintain CODD records owned by that agency.

For the Centralized Data Sharing Option, OJIN is responsible for referential integrity between the OJIN Index record and the OJIN Detailed record. Agencies who implement the Centralized OJIN Detailed Data will not be responsible for creating OJIN Index Update transactions.

Standard XML record definitions do not exist for all criminal justice record types. Some standardization efforts are underway, and OJIN will implement any appropriate standards. However, OJIN and the contribution agencies will be responsible for creating XML record definitions for most record types.

## **Assumptions**

The following assumptions were made during the design of the OJIN Index and Detailed Data Update Transactions.

- ❑ OJIN is not responsible for or designed to maintain a historical record of changes to the OJIN Index records.
- ❑ Changes to the OJIN Index Records are not logged.
- ❑ The unique identifier contained within an OJIN Index Record does not necessarily identify a unique person.
- ❑ OJIN Index records with equivalent identification information do not indicate that the records refer to the same subject.
- ❑ End users do not have transactions, access, or authorization to directly maintain any data within the Centralized OJIN Index or Centralized OJIN Detailed Data.

The business rules described previously are consistent with these assumptions.



## B. OJIN CENTRAL SERVER DESIGN

There are several types of servers necessary to support the OJIN environment. These server types include application, web, file transport protocol (FTP), database, and certificate servers and represent both logical and physical server configurations. Within the OJIN network design, servers are logically grouped so that a single physical computer may be used for more than one type of server. As the OJIN network evolves multiple physical servers may be grouped physically into server clusters for scalability requirements. Finally, servers may be defined as secure servers – those servers behind the firewalls and contained within the secure LEADS network. Section D: Network Design, utilizes these various server types to design a POCP, Phase I, and Phase II OJIN network.

Each server must be capable of handling the volume of traffic/transactions that they are subjected to, and must respond reliably within time frames that are defined as being acceptable. For the POCP, the following performance requirements must be met:

- ❑ the OJIN POCP must sustain a transaction volume of 100 simultaneous users for a period of 30 minutes with an average response time of four seconds, and
- ❑ the OJIN centralized index, the index physically located on the OJIN server, must contain a minimum of one million records.

No further performance requirements have been established, at this time, for the Phase I and Phase II operation of OJIN. Performance requirements have not been established for scenarios in which the OJIN is dependent upon various agency systems to supply data for either OJIN Index or Detailed queries.

Server reliability and availability will be achieved through:

- ❑ clustering multiple machines,
- ❑ configuring multiple CPUs per machine, and
- ❑ utilizing operating system software with fail-over capabilities.

A server cluster typically consists of two computer nodes (CPUs) with access to common, replicated, or Redundant Array of Independent Disks (RAID) storage. When one node fails, the other node takes over and provides the necessary processing services. Clustering achieves exceptionally high availability via this failover capability. At this time, no availability requirements have been defined for OJIN. However, requirements for 98% availability on a per month basis are not unusual in criminal justice environments similar to OJIN. However, the availability requirement can not be higher than that required for the LEADS network or for each contributing agency. Measurements of OJIN availability must only be applied to the centralized OJIN environment, since OJIN is extremely dependent upon the availability of contributing agencies' platforms and the LEADS network.



Regardless of the type of server, the following hardware and software products are suitable for OJIN servers:

- ❑ SUN Enterprise servers running Solaris Version 2.6, 2.7, 2.8, or higher;
- ❑ HP9000 servers running HP-UX Version 10.2, 11.0, or higher; or
- ❑ X86-based (Intel-Pentium or AMD-Athlon) systems running Microsoft Windows 2000.

The following sections describe each server type, identify any additional products necessary to construct each server type, and present the necessary server configurations for the POCP, Phase I, and Phase II.

## **B.1 APPLICATION SERVER**

The OJIN central server configuration requires an OJIN application server that will provide the OJIN business logic. The OJIN application server is part of OJIN's n-tiered architecture that consists of web, application, and database servers. Application server products consist of the server and operating systems identified previously.

## **B.2 WEB SERVER**

For OJIN, a Web Server is defined to be a server that receives, creates, or forwards Web pages to authorized OJIN users. Web pages may contain the OJIN Subject Search request or present the results of an OJIN Index Query or OJIN Detailed Query to a user. Web pages are displayed on an OJIN user's workstation using a web browser - either Netscape or Microsoft Internet Explorer.

The following software products are suitable for OJIN web servers:

- ❑ Zeus Web Server Version 3.3.7 or higher;
- ❑ Netscape iPlanet Web Server Version 4.1 or higher;
- ❑ Apache-SSL for HP9000 servers running HP-UX Version 10.2, 11.0, or higher; or
- ❑ Microsoft Internet Information Server (IIS) Version 5.0 or higher for X86-based (Intel-Pentium or AMD-Athlon) systems running Microsoft Windows 2000.

The POCP requires a single web server. Phase I may expand the web server to a web cluster based upon the number of contributing agencies, number of OJIN authorized users, transaction volumes, and availability requirements. Phase II may require multiple web servers as the agencies, users, and transaction volumes increase.



## **B.3 DATABASE SERVER**

An OJIN database server is a server that contains and provides access to the OJIN Centralized Index and any contributing agency detailed OJIN data that does not reside at a participating agency location. It is responsible for updating the index and detail data upon receipt of update transactions from contributing agencies.

The following software products are preferred, but do not represent an exhaustive list for OJIN database servers:

- ❑ Oracle Version 8 or higher,
- ❑ Informix 2000 Version 9.20 or higher, and
- ❑ Microsoft SQL Server 2000.

The POCP requires a single database server, as does Phase I. Phase II requires an additional database server in the DMZ to handle all Internet or non-criminal justice agency traffic. Phase II may also require secure database servers to provide increased speed, scalability, and redundancy based upon the increase in transactions and traffic due to Internet and non-criminal justice agency users and contributing systems.

## **B.4 FTP SERVER**

OJIN uses File Transfer Protocol (FTP) Servers to transfer OJIN Index Update transactions to OJIN from an agency server and to transfer detailed data that an agency is contributing to OJIN that will be maintained on the OJIN server. The OJIN server may function as an FTP server for these data transfers. FTP, a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. Basic FTP support is usually provided as part of a suite of programs that come with TCP/IP.

It is not expected that a separate server will be required as the OJIN FTP server. FTP is available as part of the operating system software for any of the server configurations identified in Section B.

## **B.5 OJIN MAIL SERVER**

OJIN will utilize a mail server in Phase III to forward notifications to users who have OJIN subscription services. OJIN Phase III will provide a facility to allow users or agencies to receive notifications when data is updated in the OJIN index for a particular subject, a group of subjects, or a combination of subjects and data types. The OJIN mail server will not support the receipt of incoming mail, it only forwards outgoing OJIN notifications.



Because new mail server products will be forthcoming and existing products may be supported on additional platforms, a final list of mail server software is not provided. However, the following products are currently supported for the server platforms identified in Section B:

- ❑ CommuniGate Pro and InterMail Post Office for HP-UX and Solaris operating systems, and
- ❑ NTMail for Solaris and Windows 2000 operating systems.

Additional mail servers are available for these operating systems. However, these represent the common set of mail servers.

## **B.6 OJIN CERTIFICATE SERVER**

An OJIN certificate server is a server that acts as a certification authority. Certification authorities are described in Section III. The following software products are suitable for OJIN certificate servers:

- ❑ SentryCA 4.5 from Xcert Software Inc.,
- ❑ iPlanet Certificate Management System 4.2 from Netscape Communications Corp., and
- ❑ Microsoft Certificate Services included as part of a Windows 2000 server.

The POCP will have at least two certificate servers – the OJIN server and a CPD certificate server. For Phase I, the DAS certificate server will be added as the root certification authority, and all participating agencies who choose to allow OJIN users to access OJIN index or detailed data at their agency location will have a certificate server. Non-criminal justice agencies who will act as a contributing agency in Phase II will also require a certificate server.

## **C. AGENCY SERVER DESIGN**

As with the OJIN Server design, several types of agency servers are necessary to support the OJIN environment including web, FTP, database, application, and certificate servers. Agencies may logically group servers so that a single physical computer may be used for more than one type of server. As performance and scalability requirements increase, agencies may also group multiple physical computers into server clusters. OJIN currently has no authority to impose performance requirements for agency servers. However, contributing agencies should be cognizant of the impact of their configurations on the overall performance of OJIN and provide sufficient server resources to satisfactorily handle OJIN transactions.

Participating agencies will be required to select server products that are compatible with the OJIN environment. Therefore, agencies should chose server products from the products recommended for the central agency environment.



Agency server design is based upon the role of the participating agency and their choice of data sharing model. The following sections review the agency server configurations for each data sharing model and indicate any relationship between the configuration and the various OJIN phases.

## **C.1 CENTRALIZED DATA SHARING MODEL**

To support the centralized data model, agencies do not require any additional servers. However, the following conditions apply:

- ❑ if the agency is a Certification Authority, the agency must provide a certification server using the products identified in Section B; and
- ❑ an FTP server is required; however, it may be supplied by either the agency or as part of the OJIN server environment.

Because the agency is a contributing agency, it must have already have a system that functions as an application and database server. It is not necessary to replace that configuration. For this data sharing option, OJIN does not require any access to that system. However, if the agency chooses to upgrade its environment, the agency should select products from those identified in Section B.

These server requirements are valid for all OJIN phases.

## **C.2 DISTRIBUTED DATA SHARING MODEL**

For agencies that implement the distributed data sharing model, the following server types are required:

- ❑ web server,
- ❑ database server,
- ❑ application server, and
- ❑ if the agency is a Certification Authority, the agency must provide a certification server using the products identified in Section B.

It is critical that agencies who implement distributed models have sufficient server capacity to handle Subject Search queries against the distributed OJIN Index; the retrieval of distributed OJIN Detailed Data from the agency database(s); and the transformation of that information into XML record definitions or HTML web pages within reasonable performance limits. It is recommended that, minimally, each agency adhere to the same performance requirements as those established for the OJIN POCP and defined in Section B. Agencies must also have sufficient storage capacities to maintain the distributed OJIN Detailed Data. If the agency chooses to upgrade its environment, the agency should select products from those identified in Section B.



These server requirements are valid for all OJIN phases.

### **C.3 HYBRID DATA SHARING MODEL**

For agencies that implement the distributed data sharing model, the following server types are required:

- ❑ web server,
- ❑ database server,
- ❑ application server,
- ❑ if the agency is a Certification Authority, the agency must provide a certification server using the products identified in Section B, and
- ❑ an FTP server is required; however, it may be supplied by either the agency or as part of the OJIN server environment.

Because the agency is a contributing agency, it must already have a system that functions as a database and application server. It is not necessary to replace that configuration. However, if the agency chooses to upgrade its environment, the agency should select products from those identified in Section B.

These server requirements are valid for all OJIN phases.

## **D. NETWORK DESIGN**

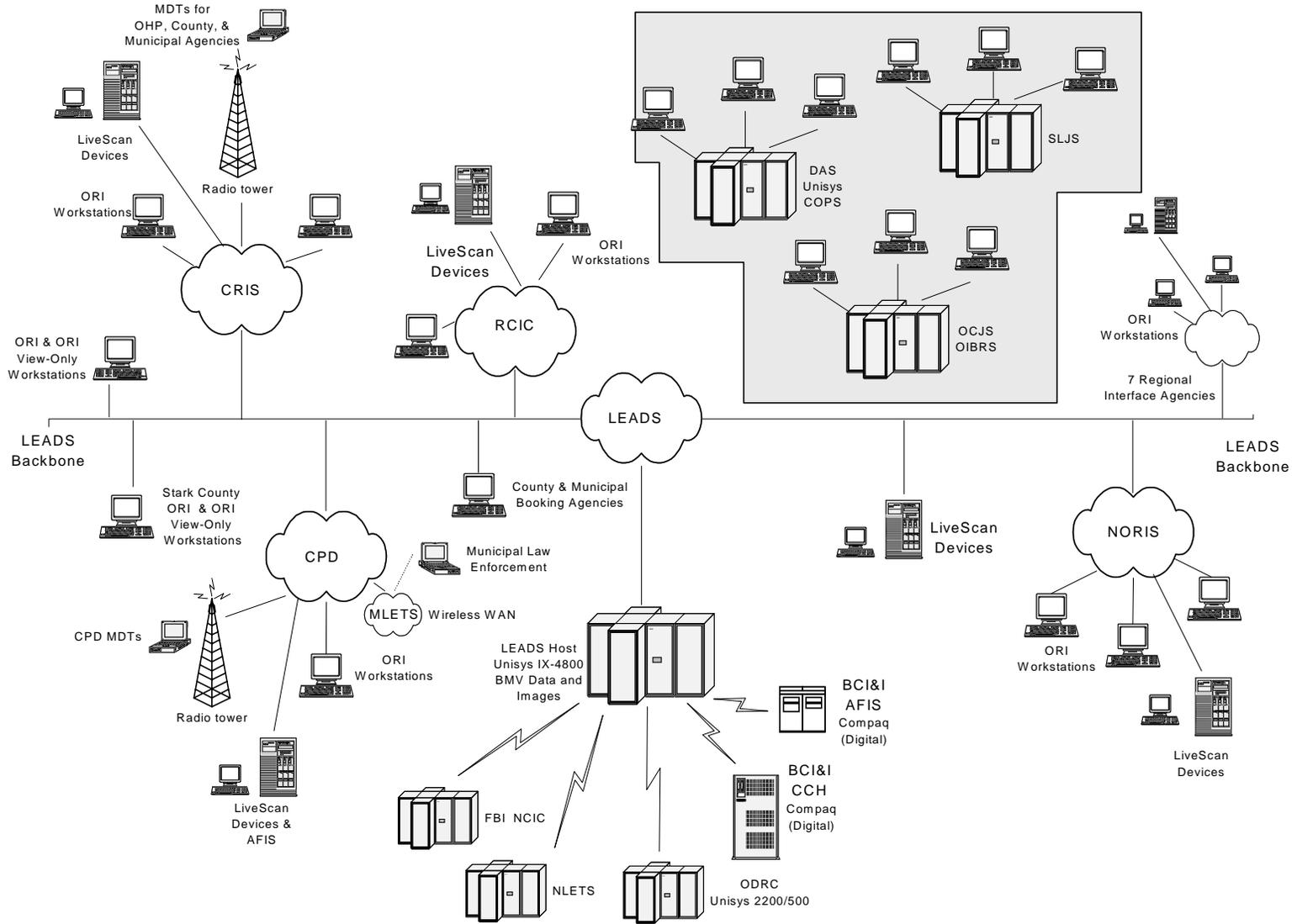
The following sections describe the transformation from the current Ohio criminal justice network environment into a OJIN POC network, followed by a functioning and secure Phase I network, and concluding with a Phase II network based upon the LEADS network.

### **D.1 CURRENT OHIO CRIMINAL JUSTICE NETWORK MODEL**

One of the OJIN Technical Architecture principles is to build upon the existing Ohio Criminal Justice technical architecture and infrastructure, wherever possible, without compromising the OJIN requirements. *Exhibit IV-3: Current Ohio Criminal Justice Environment*, is a representation of the Ohio criminal justice environment that is currently relevant to the OJIN. It includes:

- ❑ the LEADS network;
- ❑ Bureau of Motor Vehicles agency systems resident on the LEADS Unisys mainframe;
- ❑ Bureau of Criminal Identification and Investigation systems such as CCH resident on a Compaq (Digital) cluster, the Electronic Arrest Transmission System (EATS), and the Interstate Automated Fingerprint Identification system (IAFIS);

**Exhibit IV-3**  
**Current Ohio Criminal Justice Environment**





- ❑ Ohio Prosecuting Attorneys' Association Criminal Offense Prosecution System (COPS);
- ❑ Department of Rehabilitation and Correction's (ODRC) Departmental Offender Tracking System (DOTS);
- ❑ Office of Criminal Justice Services (OCJS) Ohio Incident-Based reporting System (OIBRS);
- ❑ Buckeye State Sheriff's Association (BSSA) Sheriff's Jail Linkage System (SLJS);
- ❑ three regional systems including:
  - Cuyahoga Regional Information System (CRIS).
  - Northwest Ohio Regional Information System (NORIS), and
  - Regional Crime Information Center (RCIC);
- ❑ eight regional interface agencies, defined as an agency network that is connected to LEADS, creating an Extranet including:
  - Columbus Police Department (CPD),
  - Lake County Communication Center (LCC),
  - Miami County Communications Center (MCCC),
  - Cleveland Police Department,
  - Dayton Police Department,
  - Springfield Police Department,
  - Akron Police Department, and
  - Shaker Heights Police Department.
- ❑ ORI and ORI View -only workstations;
- ❑ Mobile Data Terminals (MDTs);
- ❑ County and Municipal Booking Agencies; and
- ❑ LiveScan Devices.

The LEADS network provides access to more than 2,300 terminal locations and 1,300 mobile data terminals (MDTs). It supports 11 intrastate regional systems. LEADS also hosts direct connections to NCIC and NLETS via 56 Kbps communication lines. All LEADS workstations transfer information using the TCP/IP communications protocol over a frame relay network. Eight Cisco 7000 routers create the LEADS backbone with most of the remote connections linked with a 56 Kbps line. Cisco 2501 routers service local connections for standard LEADS workstations. LEADS workstations conform to a minimum standard of 486/66 MHz PC with 32 MB of RAM. Regional Interface Systems such as NORIS, CRIS, RCIC, and CPD are end-points of the LEADS network.



## **D.2 OJIN CRIMINAL JUSTICE NETWORK ARCHITECTURE**

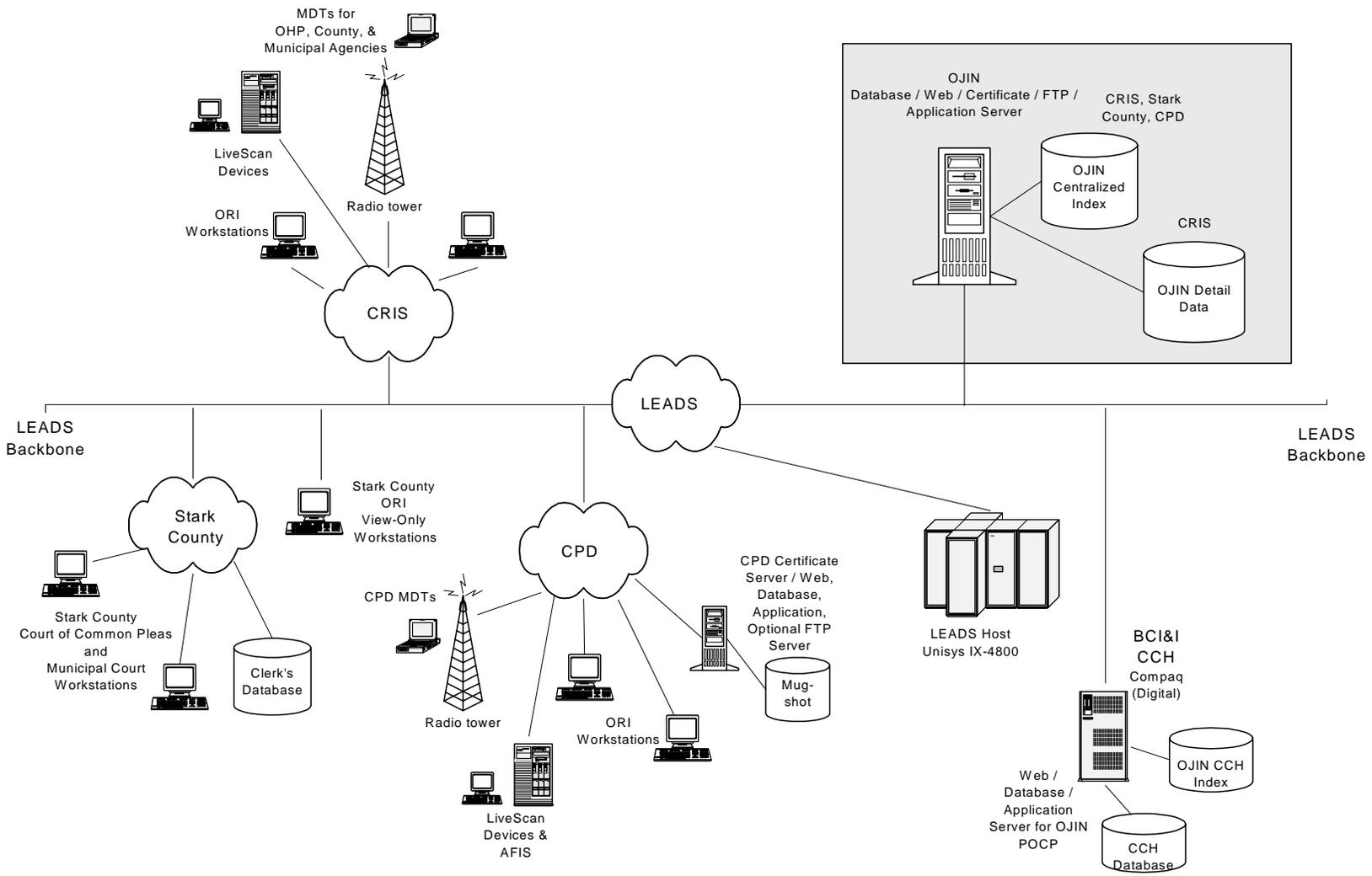
This section presents the architecture for the OJIN network. Because the OJIN will be implemented in various stages, or phases that are dependent upon factors external to this project, the network logical design is presented in a series of design stages. These stages illustrate the transformation from the current environment into a full-functioning Phase II OJIN network that permits secure access to any authorized entity. These stages are:

- ❑ Proof-of-Concept Prototype,
- ❑ Phase I, and
- ❑ Phase II.

### **D.2.1 Proof-of-Concept Prototype**

The OJIN Proof-of-Concept Prototype network logical design is based upon the existing LEADS backbone. It includes a subset of the current Ohio criminal justice environment and agencies depicted in Exhibit IV-3. *Exhibit IV-4: OJIN POCP Network Diagram*, illustrates the network environment that will be supported by the OJIN POCP. The shaded area indicates the

### Exhibit IV-4 OJIN POCP Network Diagram





only addition to the existing LEADS network, that of the OJIN server. The following participating agencies will be involved in the OJIN POCP:

- ❑ CRIS will be a contributing agency that provides arrest data to OJIN and CRIS users will have access to data provided by the other three contributing agencies,
- ❑ Stark County Court of Common Pleas and the Canton Municipal Court will provide data from the Clerks database and these court users will have access to data provided by the other three contributing agencies,
- ❑ CPD will provide CPD mugshot system data to OJIN and CPD users will have access to data provided by the other three contributing agencies, and
- ❑ BCI&I will provide Ohio CCH data to OJIN.

The OJIN server environment will be located at the Department of Public Safety in Columbus, Ohio. It consists of a server configuration as specified in Section B. The server acts as an application, database, web, and certificate server. A centralized index of the detail information provided by CRIS, CPD, BCI&I, and Stark County will be located on this server as well as the detail data provided by CRIS.

The LEADS network currently supports the following types of transactions:

- ❑ LEADS transactions originated from ORI (Originating Agency Identifier) workstations, and
- ❑ IAFIS transactions from Live Scan workstations.

With the addition of the OJIN POCP, the LEADS network will also transport:

- ❑ OJIN Detailed Query transactions that contain requests for and responses of detailed data among contributing agency workstations (subset of LEADS ORI and MDT devices, referred to as OJIN workstations), OJIN servers, and contributing agency servers;
- ❑ OJIN Index Query transactions between OJIN and BCI&I;
- ❑ index maintenance transactions from contributing agencies (CPD, CRIS, Stark County) to OJIN; and
- ❑ detailed data maintenance transactions from CRIS.

The POCP will not add any new ORI workstations to the LEADS network. OJIN POCP workstations will be any authorized LEADS or a CRIS or CPD workstation that is connected to LEADS through existing regional networks. The OJIN environment will use TCP/IP communications protocol over the LEADS frame relay network connecting via the existing routers at the Department of Public Safety.



The routers that currently handle ORI traffic between LEADS and the various ORI workstations or regional Extranets will be re-configured to route LEADS traffic to LEADS servers and OJIN traffic to the OJIN server.

## Assumptions

The following assumptions were made in order to define the POCP network environment.

- ❑ OJIN transactions between BCI&I and OJIN will not be routed through the LEADS Unisys mainframe. OJIN transactions will be routed directly between BCI&I and OJIN.
- ❑ The CRIS and CPD Extranets are trusted, secure networks.
- ❑ BCI&I will return data from an OJIN Index query according to the pre-defined OJIN XML Index Query format. BCI&I can choose to respond to OJIN Detailed Queries either using the OJIN Detailed Query XML format or using static HTML pages.
- ❑ OJIN will act as its own certificate authority, 3<sup>rd</sup> party certificate authorities will not be utilized.

If these assumptions change, the network logical design must be updated to accommodate the change.

## D.2.2 Phase I

For Phase I the OJIN network is extended to include additional contributing or non-contributing criminal justice agencies. Workstations owned by criminal justice agencies are also included in the OJIN environment. OJIN Phase I supports the same types of transactions as does the POCP. All OJIN devices will continue to communicate using TCP/IP. *Exhibit IV-5: POCP to Phase I Network Comparison*, summarizes the network differences between the POCP and Phase I.

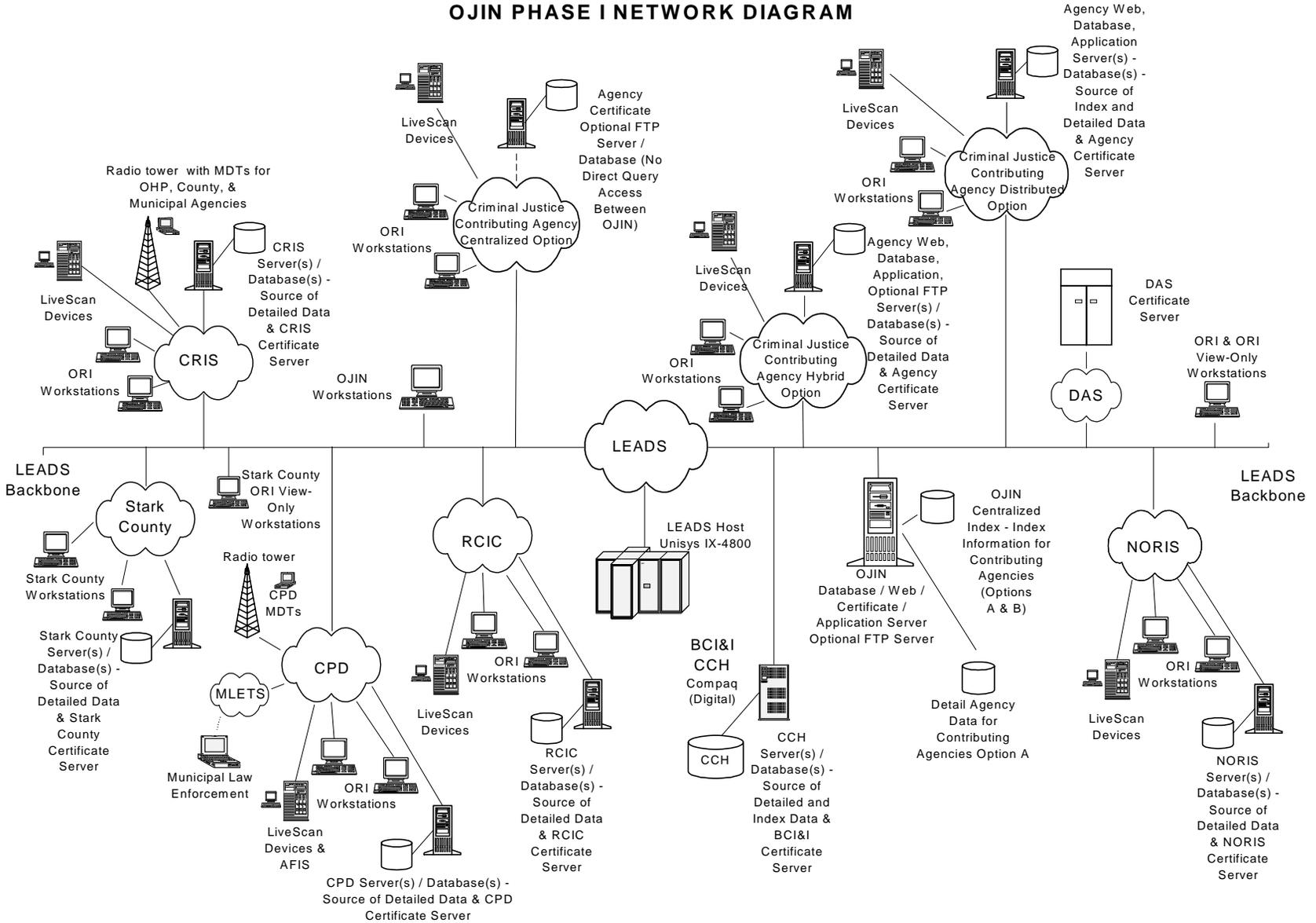


**Exhibit IV-5  
POCP TO PHASE I NETWORK COMPARISON**

<b>Category of Change</b>	<b>POCP</b>	<b>Phase I</b>
Participating Agencies	BCI&I CRIS CPD Stark County	Any Criminal Justice Agency
Workstations	Any workstation owned by LEADS which conforms to the minimum configuration specified in Section F	Any workstation owned by a criminal justice agency which conforms to the minimum configuration specified in Section F
Extranets	CRIS CPD	Any Extranet owned by a criminal justice agency (agencies with authorized ORI workstations and users)
Routing	Routers are configured to appropriately route LEADS and OJIN traffic	Routers are re-configured to route OJIN traffic between additional Phase I Extranets / workstations and OJIN servers
Firewalls	None Required	None Required
Network Protocol	TCP/IP	TCP/IP
Servers	CPD Server(s): <input type="checkbox"/> Web, <input type="checkbox"/> Application, <input type="checkbox"/> Database, <input type="checkbox"/> FTP (optional), and <input type="checkbox"/> Certificate. BCI&I Server(s): <input type="checkbox"/> Web, <input type="checkbox"/> Application, and <input type="checkbox"/> Database. Stark County Server(s): <input type="checkbox"/> Web, <input type="checkbox"/> Application, <input type="checkbox"/> optional FTP, and <input type="checkbox"/> Database. OJIN Servers <input type="checkbox"/> Web, <input type="checkbox"/> Application, <input type="checkbox"/> Database, <input type="checkbox"/> FTP (optional), and <input type="checkbox"/> Certificate.	Additional contributing Criminal Justice Agency Servers in addition to those specified for the POCP <input type="checkbox"/> Web, <input type="checkbox"/> Application, <input type="checkbox"/> Database, <input type="checkbox"/> FTP (optional), and <input type="checkbox"/> Certificate.

*Exhibit IV-6: OJIN Phase I Network Diagram*, illustrates the logical design for the Phase I OJIN network. Refer to Section III, subsection D for a description of the contributing agency options.

### Exhibit IV-6 OJIN PHASE I NETWORK DIAGRAM





As long as the OJIN system continues to operate using the LEADS network and all agencies (contributing and non-contributing) are drawn from the pool of agencies who are authorized ORI terminal users, no additional network hardware will be required. Workstations or Extranets can be treated as either ORI workstations or Regional Interface Systems respectively, as illustrated in Exhibit IV-6.

## Assumptions

The following assumptions were made in order to define the Phase I network environment.

- ❑ OJIN transactions between BCI&I and OJIN will not be routed through the LEADS Unisys mainframe. OJIN transactions will be routed directly between BCI&I and OJIN.
- ❑ All criminal justice agency Extranets that will be connected to the LEADS backbone in Phase I are authorized, trusted, and secure networks.
- ❑ All workstations that will be connected to the LEADS backbone in Phase I are authorized ORI workstations.
- ❑ DAS will become the root CA, OJIN will become a subordinate certificate authority, and criminal justice agencies must assume certificate authority for authorized users within their jurisdiction.

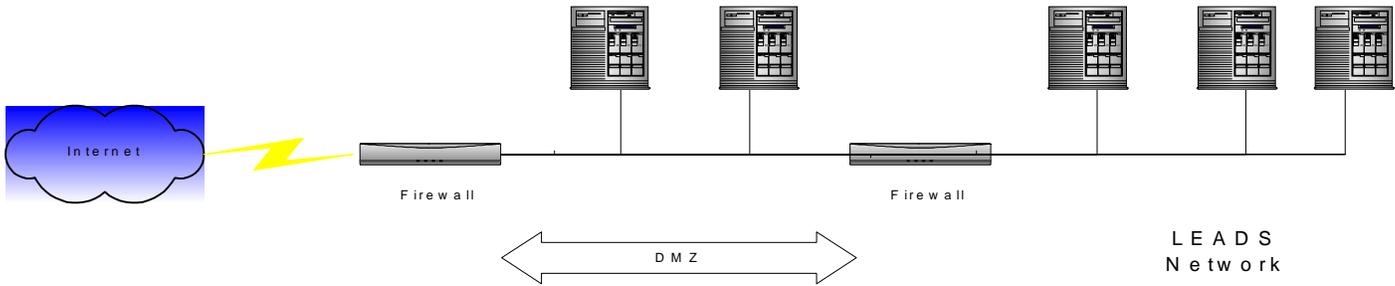
If these assumptions change, the network logical design must be updated to accommodate the change.

### D.2.3 Phase II

For Phase II the OJIN network is extended to include additional contributing or non-contributing non-criminal justice agencies and users. Extension of the OJIN in this manner will require considerable network changes in terms of firewalls, Demilitarized Zones (DMZs), and the LEADS network itself. *Exhibit IV-7: High-Level OJIN Phase II Network Configuration*, illustrates a very high level view of the network changes necessary for OJIN Phase II. The changes are identified as the DMZ in Exhibit IV-7.



**Exhibit IV-7  
HIGH-LEVEL OJIN PHASE II NETWORK CONFIGURATION**



*Exhibit IV-8: Phase I to Phase II Network Comparison*, summarizes the network differences between Phase I and Phase II.



**Exhibit IV-8  
PHASE I TO PHASE II NETWORK COMPARISON**

<b>Category of Change</b>	<b>Phase I</b>	<b>Phase II</b>
Participating Agencies	Any Criminal Justice Agency	Any Agency authorized by the OJIN Governance Structure
Workstations	Any workstation owned by a criminal justice agency which conforms to the minimum configuration specified in Section F	Any workstation owned by an agency authorized by the OJIN Governance Structure – this could be interpreted to mean users as varied as the public and which conforms to the minimum configuration specified in Section F
Extranets	Any Extranet owned by a criminal justice agency (agencies with authorized ORI workstations and users)	Any network belonging to any entity authorized to access the OJIN
Routing	Routers are configured to appropriately route LEADS and OJIN traffic	Routers are configured to appropriately route LEADS and OJIN traffic
Firewalls	None required	Two firewalls and a DMZ are required for each Internet Service Provider (ISP) point-of-presence for access by non-criminal justice agencies.
Network Protocol	TCP/IP	TCP/IP
Servers	Criminal Justice Agency Servers <ul style="list-style-type: none"> <li><input type="checkbox"/> Web,</li> <li><input type="checkbox"/> Application,</li> <li><input type="checkbox"/> Database,</li> <li><input type="checkbox"/> optional FTP, and</li> <li><input type="checkbox"/> Certificate.</li> </ul> OJIN Servers <ul style="list-style-type: none"> <li><input type="checkbox"/> Web,</li> <li><input type="checkbox"/> Application,</li> <li><input type="checkbox"/> Database,</li> <li><input type="checkbox"/> optional FTP, and</li> <li><input type="checkbox"/> Certificate.</li> </ul>	OJIN Servers in addition to those types specified for Phase I, which may include: <ul style="list-style-type: none"> <li><input type="checkbox"/> Web Clusters (groupings of web servers)</li> <li><input type="checkbox"/> Server clusters (groups of application and / or database / FTP servers),</li> <li><input type="checkbox"/> Secure Database server, and</li> <li><input type="checkbox"/> Secure Server clusters.</li> </ul>

*Exhibit IV-9: OJIN Phase II Network Design*, is a representation of the Phase II OJIN logical network design. It illustrates two new types of access:

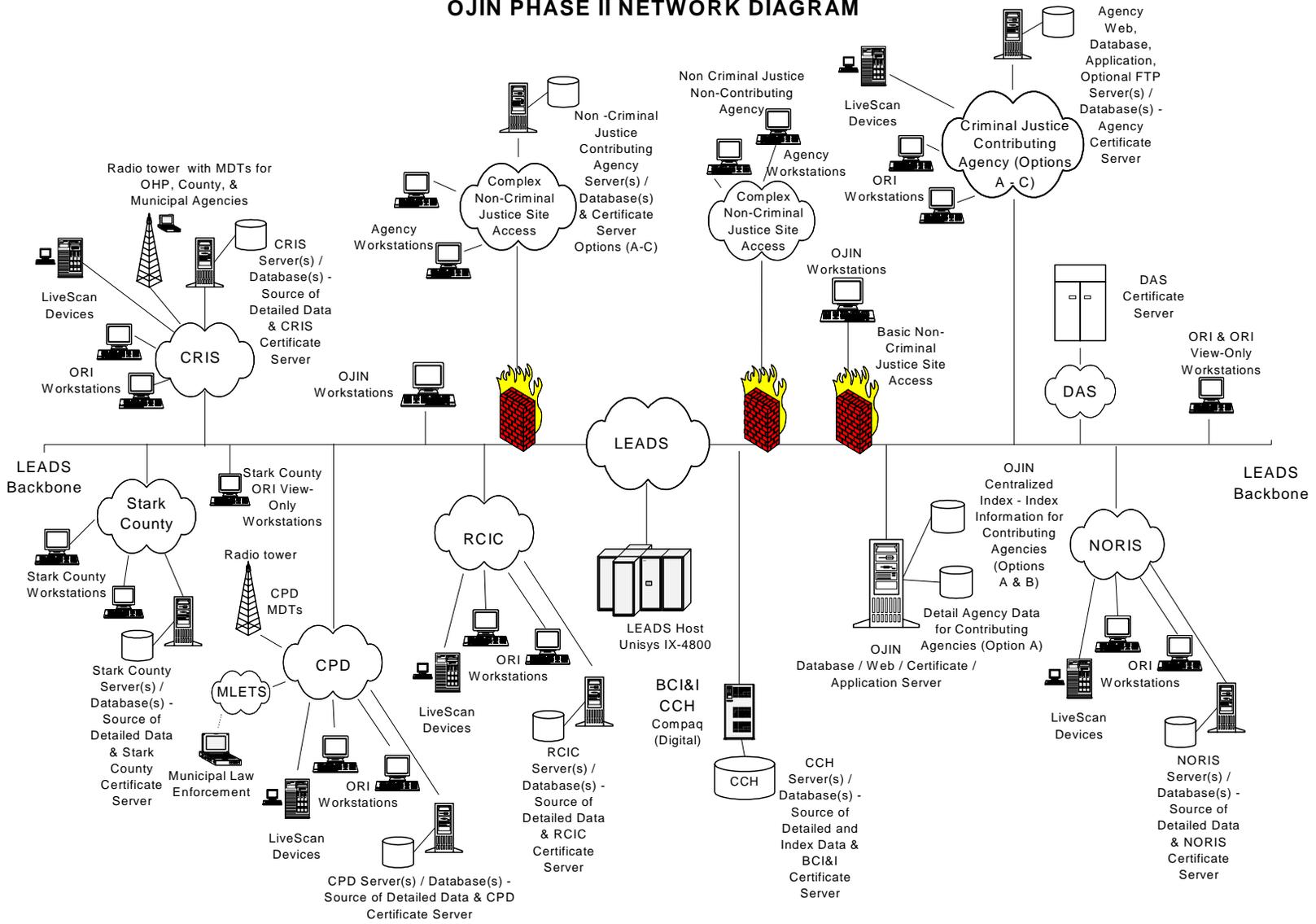
- Basic Non-Criminal Justice Site access, and
- Complex Non-Criminal Justice Site access.

These access types are discussed in the following sections.

**Assumptions**

The following assumptions were made in order to define the Phase II network environment.

### Exhibit IV-9 OJIN PHASE II NETWORK DIAGRAM





- Agencies, organizations, entities, and users who are not authorized ORI users may be authorized to access OJIN.

The following sections provide a detailed discussion of the network changes required to achieve Phase II functionality and product recommendations for each new OJIN Phase II network component.

### D.2.1.1 Basic Non-Criminal Justice Site Access

*Exhibit IV-10: Basic Non-Criminal Justice Site Access to OJIN*, illustrates a network configuration that can be used to provide secure OJIN access to non-criminal justice agencies, sites, or users via the Internet, represented in Exhibit IV-10 as a cloud. This configuration would typically be used to support smaller OJIN traffic loads received from authorized users. It does not provide high levels of scalability or availability.

**Exhibit IV-10  
BASIC NON-CRIMINAL JUSTICE SITE ACCESS TO OJIN**

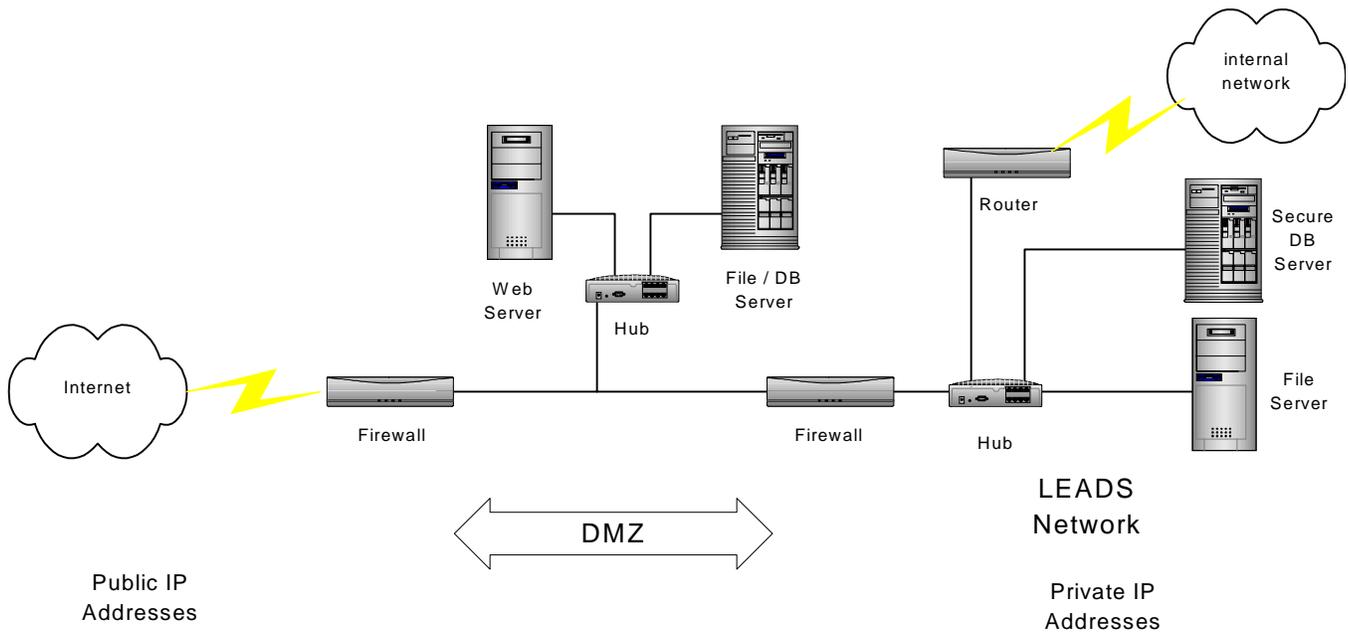


Exhibit IV-10 identifies several components which are necessary to provide access to Internet users. The server components have been described previously in Section B: OJIN Central Server Design, and firewall components are described in Section E: OJIN Security Design. The equipment needed to implement the OJIN Basic Non-Criminal Justice Site access includes:



- **File / Web / Database Servers**– Suitable products include:
  - SUN Enterprise Servers with Solaris V2.6 or higher,
  - HP9000 servers with HP-UX 10.2 or higher, or
  - X86-based (Intel-Pentium or AMD-Athlon) systems with Windows 2000.
- **Web Server Software** – Suitable products include:
  - Apache-SSL,
  - Zeus Web Server 3.3.7 or higher,
  - Netscape iPlanet Web Server 4.1, or
  - Microsoft Internet Information Server (IIS) 5.0 or higher.
- **Database Server Software** – Suitable products include:
  - Oracle Version 8 or higher,
  - Informix 2000 Version 9.20 or higher, and
  - Microsoft SQP Server 2000.
- **Hubs/Switches/Firewalls/Routers** – Suitable vendors include:
  - Cisco,
  - 3Com,
  - Cabletron,
  - Lucent, and
  - Hewlett-Packard.

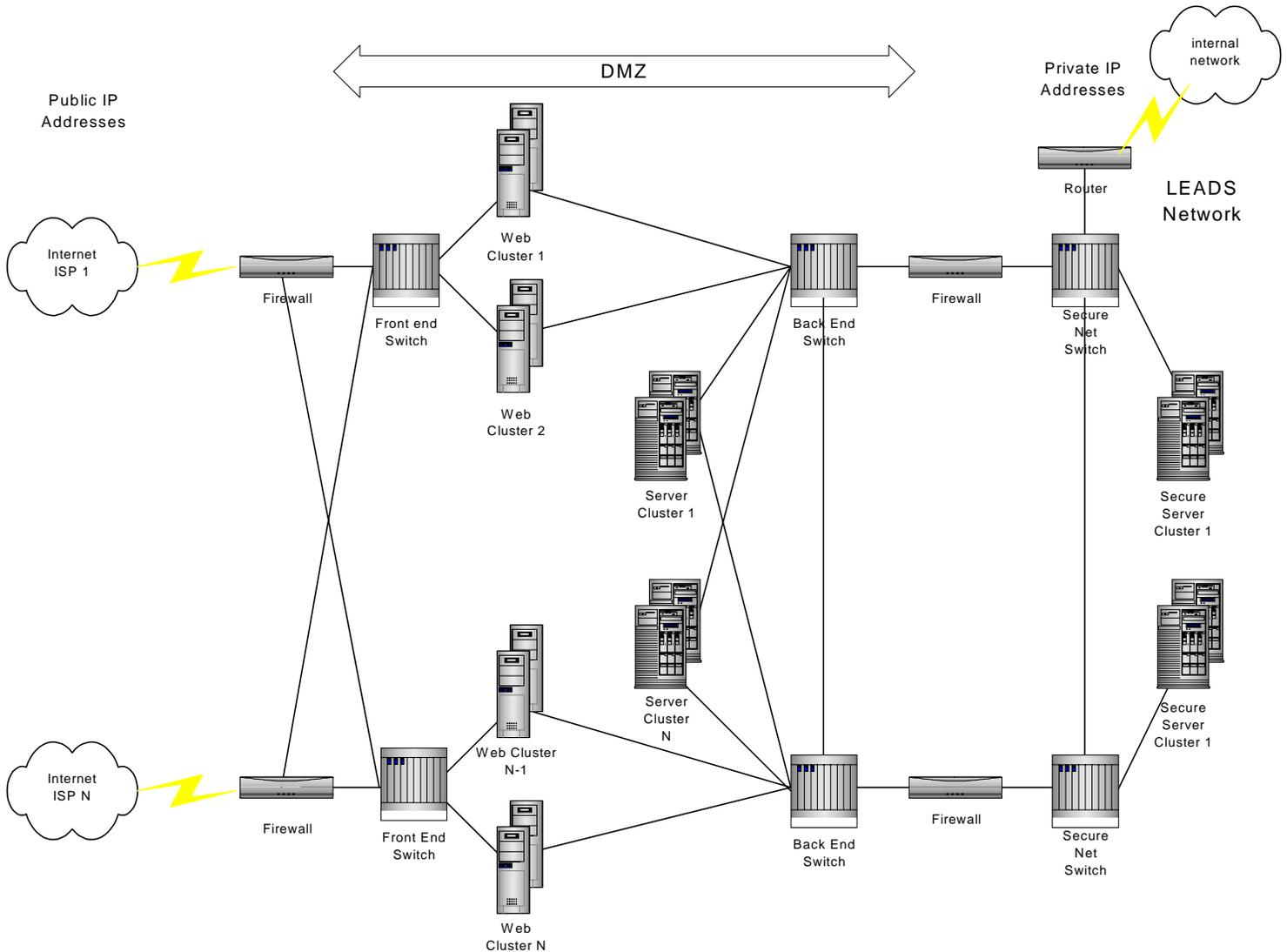
Selection of the appropriate network hardware should be made only after considering other factors such as network speeds, manageability, supported protocols, and number of ports which cannot be determined until detailed design of OJIN Phase II begins.

### **D.2.1.2 Complex Non-Criminal Justice Site Access**

*Exhibit IV-11: Complex Non-Criminal Justice Site Access to OJIN*, illustrates a network configuration to provide secure OJIN access via the Internet that supports large amounts of OJIN traffic, scalability requirements, and high availability through redundant configurations. There are no functional differences between the services available through the Basic Non-Criminal Justice Site Access and the Complex site access.



## Exhibit IV-11 COMPLEX NON-CRIMINAL JUSTICE SITE ACCESS TO OJIN



Equipment needed to implement secured OJIN access using the Complex Non-Criminal Justice Site access is the same as that recommended for Basic Non-Criminal Justice Site Access in Section D.2.1.1.

### Assumptions

Requirements for performance, scalability, and redundancy based upon the increasing volume of Internet traffic drive the decision to move from a Basic Non-Criminal Justice Access model to the Complex Non-Criminal Justice Site access configuration.



## E. OJIN SECURITY DESIGN

Security of OJIN resources - hardware, network and data, can be provided by:

- ❑ restricting physical access to OJIN hardware;
- ❑ controlling network traffic through the use of routers/firewalls and creating demilitarized zones (DMZs); and
- ❑ limiting access to data through authentication, access control lists and encryption.

Restriction of physical access to OJIN equipment must be the responsibility of the agency where the equipment is located. For at least the POCP, physical access security will be the responsibility of the Department of Public Safety.

Network traffic is primarily controlled through the use of routers. Routers are hardware devices/software that connect two or more networks. They accept packets on at least two network interfaces, and forward packets from one interface to another. When they are programmed to filter out some packets by examining packet type as well as source and destination addresses, they act as firewalls. Routers that have one or more interfaces to the Internet must support the Border Gateway protocol. Network hardware companies such as Cisco, 3Com, Nortel, and Lucent are well-known manufacturers of routers. Exhibit IV-9 illustrates the application of these concepts to the Phase II OJIN network.

Authentication of users is achieved through login dialogs and through the verification of certificates against certificate trust lists. The use of X.509v3 certificates and corresponding Certificate Management Software will handle user authentication through web servers and web browsers. Certificate server software from XCert Software, Netscape Communications, or Microsoft; web server software from Apache, Zeus, Netscape, or Microsoft; and web browser software from Netscape or Microsoft satisfies these requirements.

Access control lists provide a means to match user credentials against predefined rules that determine whether the authenticated user is granted privileges to view, add, modify, or delete OJIN data. Access control lists will be handled through application software and made available through web browser interfaces.

Encryption provides safeguards against eavesdropping and modification of data. The Secure Hyper-Text Transfer Protocol (HTTPS) uses Secure Sockets Layer (SSL) to encrypt information between a web server and web browsers. A digital certificate must be installed on the web server for it to communicate using HTTPS. While HTTPS and SSL work at the server and browser level, another form of encryption, IPSec, encrypts all TCP/IP traffic between two end-points on a network. HTTPS and SSL support requires the use of digital certificates and is provided by web server software supporting certificates. Current versions of web browser software from Netscape and Microsoft also support certificates. IPSec support is usually at the operating system level and, in Microsoft products, is available only on the Windows 2000 products.



*Exhibit IV-12: OJIN Security Architecture*, summarizes the security mechanisms that must be implemented for each OJIN stage.

**Exhibit IV-12  
OJIN SECURITY ARCHITECTURE**

	<b>POCP</b>	<b>Phase I</b>	<b>Phase II</b>
Physical Security	√	√	√
Routers	√	√	√
Firewalls			√
Certificates	√	√	√
Encryption – HTTPS and SSL			√
Encryption – IPSec			√

It should be noted that, although firewalls are highly recommended for Phase II, firewalls can be deployed as early as the POCP. Similarly, HTTPS and SSL encryption is available in all recommended web server software products and can be implemented in any OJIN phase. IPSec encryption can likewise be implemented in any phase for servers executing Windows 2000. However, if IPSec is implemented on any Windows 2000 servers, it should be noted that the SSL/HTTPS encryption is an additional layer of encryption, since IPSec is implemented at a lower level.

**F. USER DEVICE SPECIFICATIONS**

The OJIN Architecture places a limited number of constraints on workstations selected for use as OJIN devices. These requirements are indicated below:

- ❑ A user device must employ a “thin client” strategy to function as an OJIN workstation. Querying workstations must be capable of running browser-based client software. Since workstation price/performance ratios continue to improve rapidly, exact specifications and procurement of new workstations should be done just-in-time for rollout.
- ❑ OJIN workstations should preferably have 17-inch monitors and must have a network adapter compatible with the agency or LEADS network.
- ❑ Browser software must be capable of handling X.509v3 digital certificates; current industry-leading browser software from either Netscape or Microsoft satisfies that requirement.
- ❑ If IPSec is chosen as an encryption protocol, server and workstation operating systems must be capable of supporting it. Currently, within Microsoft’s offerings, only the Windows 2000 family supports IPSec.



It is expected that many existing workstations within the criminal justice agencies can be used as OJIN workstations.

## **G. APPLICATION DESIGN ARCHITECTURE**

The following list of design principles has been developed to guide the design and implementation of the OJIN web page design.

- ❑ OJIN web pages can be displayed using either Netscape Navigator Version 4.0 or higher or Microsoft Internet Explorer Version 4.0 or higher.
- ❑ OJIN web pages will use standard and consistent presentation styles for identification and ease of use.
- ❑ The page design should compress redundant data and should limit size of retrieved data to groups of 10 results at a time.
- ❑ OJIN web pages will include a standard a navigation header with links to the OJIN Home Page, Subject Search (start a new search), and Help. Additional navigation links such as previous/next record, will be added when appropriate. Links will be located in the same area on all navigation headers.
- ❑ OJIN web pages will include an informational footer identifying the date and time it was created.
- ❑ OJIN standard images will be small for fast loading and minimum caching. Images will have alternate text to support non-graphical browser options.
- ❑ Color may be used to highlight information, but no information will be represented solely by color - additional text or image clues will assist color-blind users.
- ❑ Text size and fonts will be set by the user's browser preferences.
- ❑ No cookies will be stored on the client PCs. If user preferences are to be maintained they will be tracked by the user's certificate.

OJIN will use Active Server Page (ASP) scripts to create web pages. All database access and code execution will occur on a server. No applets will run on client machines. The ASP scripts will combine:

- ❑ JavaScript as the programming language,
- ❑ Database access,
- ❑ XML formatted data,
- ❑ Document Type Definitions (DTD) that describe XML data, and
- ❑ Extensible Style Language (XSL) to ensure uniform display.



The result will be standard HTML pages that can be displayed in Netscape Navigator 4 or Microsoft Internet Explorer 4.

The following web pages have been designed to support the OJIN query transactions and conform to these design principles. *Exhibit IV-13: Query Criteria for Subject Search*, provides a sample layout for users to enter query criteria for a subject search. The web page sample includes criteria entered to search for an individual whose name is Edward Fabeetz. It illustrates the availability of the following search options:

- demographic information,
- soundex* for first and last name,
- age range,
- subject identifiers,
- search by region, and
- search specific types of information.



## Exhibit IV-13 QUERY CRITERIA FOR SUBJECT SEARCH

STATE OF OHIO  
OHIO JUSTICE INFORMATION NETWORK  
OJIN

Subject Search      User Preferences      Help

**Search for**

Last Name: FABEETZ      SOC#

First Name: EDWARD      FBI #

Middle Name       Soundex      BCI #

Sex: Male      Race: White      License #

Age: 40 +/- 5 years      DOB

**In regions**

Northwest     Northeast     Central     Southwest     Southeast

**Include**

Booking     Criminal Cases     Criminal History     Mug Shot

Submit Query

OJIN Name Search 04 JAN 2001 1999

*Exhibit IV-14: OJIN Index Search Results*, provides a sample listing of results found by a theoretical search according to the parameters in Exhibit IV-13. It illustrates each distinct group of offender identifiers, the four Fabetz lines indicating different values of Social Security Number, FBI number, and BCI identifier, and lists the available detail records - the 10 numbered cases or bookings. Following the list are *links* to additional sets of ten results. The search criteria are displayed again to allow the user to narrow or change the search, depending upon the results. Clicking on the detail record presents the full detail record data.



## Exhibit IV-14 OJIN INDEX SEARCH RESULTS

The screenshot shows a Microsoft Internet Explorer window titled "OJIN Subject Search - Microsoft Internet Explorer". The address bar shows "http://discovery/ojin\_search03.html". The page content includes the "STATE OF OHIO" logo and "Ohio Justice Information Network" text. There are navigation links for "Subject Search", "User Preferences", and "Help".

Below the navigation links, it states "46 Records Found". A table displays search results with columns: Name, DOB, Sex, Race, SOC#, FBI#, and BCI#. The first record is for "FABEETZ, Edward G." with DOB 12/07/1961, Sex M, Race W, and SOC# 292-12-3456. Below the table, there are numbered links (1-10) for each record, such as "1 Booking 20000814002, 08/14/2000 Flag Burning, Released 08/20/2000".

At the bottom of the search results, there is a "Search for" section with input fields for Last Name (FABEETZ), First Name (EDWARD), Middle Name, Sex (Male), Race (White), SOC#, FBI#, BCI#, and License #. There is also a "Soundex" checkbox.

*Exhibit IV-15: OJIN Detail Information*, shows a sample layout of detailed case information. The actual data displayed will depend on the XML definition for each record type. This sample shows the navigation to each row in the current result set and to each result set. Again, the search criteria is displayed to allow the user to narrow or change the search.



## Exhibit IV-15 OJIN DETAIL INFORMATION

The screenshot shows a Microsoft Internet Explorer window titled "OJIN Subject Search - Microsoft Internet Explorer". The address bar contains "http://discoverj/ojin\_search04.html". The page content includes a header for the "STATE OF OHIO" and "OJIN" with navigation links for "Subject Search", "User Preferences", and "Help".

The main content area displays case details for Case# CRB-97-10267-0101, Status: Closed, Filed: 07/15/1997. The charge is 509.08 ORC M4 LOITERING. The defendant is FABEETZ, Edward Xavier, DOB: 08/11/1959, Sex: M, Race: White. Arrest Agency: Mayberry Police, Arrest Date: 07/15/1997 02:00, Location: 10THMAINMAYBERRY. Other details include SOC: 292-89-1234, BCID: B986532, FBI#: 772389EA5, and Complainant: Andy Taylor.

Below the case details is a "Case Docket" section with a table of entries:

Date	Docket Text
01/29/1998	Entries prior to this were converted from the old computer system.
01/29/1998	Days Suspended/Cred.
01/29/1998	Defendant sentenced to 030 days in an unknown facility suspended sentence. 030 days suspended.
01/29/1998	Sentence hearing.
01/29/1998	Defendant found guilty by judge.
01/29/1998	Defendant enters plea of no contest.
01/29/1998	Arraignment held.
01/13/1998	At the request of Defense, case continued. See case file for reason.
01/13/1998	Arraignment held.
01/11/1998	Federal Court Order bond posted.
01/11/1998	Bond set as Federal Court Order.
01/11/1998	Served, warrant returned.
05/26/1997	Bond set.
05/26/1997	Bench warrant issued.
05/26/1997	Arraignment held.

At the bottom, there is a search bar with "Last Name" set to "FARFFT7" and "SOC#". A "Trusted sites" icon is visible in the bottom right corner.

Agencies that implement the Distributed or Hybrid Data Sharing models may choose to return the detailed data as HTML pages to the OJIN server. In this instance, OJIN does not control the format or style in which the detailed data is displayed. OJIN simply displays the HTML page as formatted by the agency system. This option will typically be used by agencies who utilize browser-based presentations for their existing systems.