State of Wisconsin Department of Transportation
Bureau of Highway Operations

Traffic Operations & Public Safety
Communications Interoperability Assessment & Plan

Data Interoperability
Conceptual Design

March 2005

WISCONSIN DEPARTMENT OF TRANSPORTATION
TRAFFIC OPERATIONS AND PUBLIC SAFETY
COMMUNICATIONS INTEROPERABILITY ASSESSMENT AND PLAN
Data Interoperability
Conceptual Design

Table of Contents

WISCONSIN DEPARTMENT OF TRANSPORTATION
TRAFFIC OPERATIONS AND PUBLIC SAFETY
COMMUNICATIONS INTEROPERABILITY ASSESSMENT AND PLAN

Data Interoperability Conceptual Design

1. Introduction

Using a structured system engineering approach, the WisDOT Traffic Operations and Public Safety Communications Interoperability Assessment and Plan project studied the needs for data interoperability among Public Safety and transportation agencies in the State of Wisconsin. The system engineering approach enabled the project team to advance the general concept of data interoperability into a very specific set of functional requirements. This approach, along with the analysis of needs, and the definition of requirements, are presented in the project report titled "Report on Table Top Sessions and Data Interoperability Requirements". The functional requirements that were identified, along with the necessary support infrastructure, are collectively labeled the "Incident Information Exchange" system, or IIE system.

This report takes the IIE system requirements a step further towards a tangible outcome by presenting a conceptual design for the system. A subsequent Implementation Plan report will identify the steps to implement and deploy the system.

Full implementation of the IIE system will require a highly cooperative environment among public safety and transportation agencies. Homeland security awareness and initiatives, and the need for voice interoperability, as a precursor to data interoperability, have lead to significant recent improvements in inter-agency cooperation in the Public Safety sector. Overall, we see this trend of improved cooperation moving in the right direction.

Implementation of the IIE system will also require an extensive state-wide communications infrastructure and considerable financial resources. Under the current state financial constraints, development and deployment of a communications infrastructure dedicated for IIE system use would be difficult to justify. For the implementation of the IIE system to be cost effective, the needed data communications capabilities should be leveraged from the shared use of infrastructure already serving, or planned to serve, other state-wide needs, or by funding incremental enhancements to these existing or planned shared infrastructures. For example, it is far more cost-effective to consider IIE system mobile data needs in the evolution of the State Patrol's existing mobile data system, than to attempt to deploy a parallel state-wide mobile data system dedicated to IIE system use.

Availability of funding, the pace of infrastructure development, and the challenges of interagency cooperation dictate a long planning horizon for full deployment of the IIE system (e.g. 5 -

10+ years). The conceptual design presented in this report is consistent with the likelihood of a protracted deployment. The design attempts to take maximum advantage of existing public and private infrastructures, and can be deployed incrementally.

This Conceptual Design Report is organized as follows:

- Section 2 presents an overview of the IIE system concept and functional requirements.
- Section 3 summarizes the IIE system requirements that impact the conceptual design. These requirements establish the design criteria.
- Section 4 identifies and describes infrastructure that already exists in the state that could be used as resources for the IIE system design.
- Section 5 describes the industry trends in wireless data and other technologies that are relevant to the IIE system design. Because of the long planning horizon, it is prudent to consider these advancements, and not constrain the design to current technology.
- Section 6 presents the conceptual design for the IIE system hardware configuration and software architecture.

2. IIE System Overview

Table Top sessions were conducted in each WisDOT district to bring together members of the Public Safety and transportation communities to discuss and identify requirements for data interoperability. The ability for agencies to exchange data is only half the equation for achieving data interoperability. For the exchanged data to have full value, it must also be interpreted and presented to the users as usable information. Analysis of the Table Top sessions identified a set of functions to achieve this objective. These functions, along with the necessary software, computer systems, end-user devices, and communications infrastructure were identified collectively in the Data Interoperability Requirements Report as the "Incident Information Exchange" system, or IIE system.

2.1 Information Exchange Hub

The data interoperability functions identified from the Table Top sessions, can be implemented in one of two basic system architectures:

- Pure data can be exchanged between neighboring agencies and each agency can develop its own applications to utilize that data, or
- Each agency can exchange data indirectly, through a "hub". This information exchange hub can also provide the desired functionality for processing and presentation of that data.

Data interoperability between Wisconsin Public Safety and Highway Operations-related agencies can involve literally hundreds of agencies. Under the first architecture scenario, a mesh network of point-to-point connections between agencies, with each agency developing its own applications would be extremely expensive, very difficult to implement, and enormously challenging to manage.

The second, "hub" architecture is a far more achievable approach to accomplishing the desired data interoperability and functionality. Under this scenario, the IIE system will need to serve as the hub for interagency communications. As such, the IIE system will need to interface to these agencies and the computer systems these agencies use to support realtime operations. The hub will also house the interoperability applications that will process the data acquired from the interagency links, and present the data as useful information to the system users. This hub approach is illustrated in Figure 2.1-1 below.

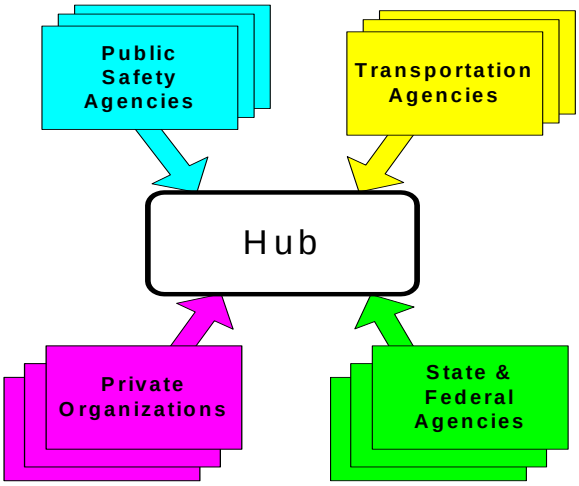

Figure 2.1-1
IIE System – Information Exchange Hub

2.2 IIE System Functions

Analysis of the Table Top Sessions identified the following functions for the IIE System. Please refer to the "Report on Table Top Sessions and Data Interoperability Requirements" for additional detail on each requirement.

a. User Interface: The user interface for the IIE system should be simple, intuitive, sensitive to connection speed, and tailored to the display and entry capabilities of the user's computer equipment. Special features, such as voice to text, should be provided for field users operating in a wireless mobile data environment.

b. Contacts: The IIE system should include a comprehensive contact database, searchable by multiple criteria, including specific individuals, expertise, geographic region, and position within an agency.

c. Alerts and Notifications: IIE system users should be able to send alerts to responders that a situation has occurred that requires their attention or awareness. Users should also be able to send notifications to specific individuals or groups about situations that they should be aware of that might impact their daily routine, or may become relevant in a highway emergency.

d. Resource, Action, and Information Requests: Users should be able to request a resource or a specific action be taken by another agency in responding to an incident. A user should also be able to request information from another agency. The IIE system should provide the mechanisms to alert the user and track that the request has been received and is being acted upon.

e. Messaging: Participants in an incident should be able to send text messages to each other directly, or in a "Chat Room" environment.

f. Incident Log: All information exchanged about an incident should be inserted into the Incident Log.

g. Whiteboard: A collaborative whiteboard function should provide a "blank sheet" for an incident commander or other participant to present a situation in text or sketch form simultaneously to all incident participants.

h. Preprogrammed Protocols: The IIE system should include utilities and functions to import, develop, access, and execute preplanned incident responses.

i. Access to Traffic Information: Information from existing and evolving traffic management systems should be accessible to all users. This information should include camera video and control, traffic flow data, VMS sign location and display, road weather conditions, road construction plans, and plans for day-to-day highway maintenance activities.

j. AVL: An Automatic Vehicle Location function should be provided for agencies that desire this capability. The function should display the location of incidents and incident responders on a map display, and be tightly integrated with other IIE system functions.

k. Reference Material: Users of the IIE system should be able to quickly access reference material, such as manuals, procedures, maps, and drawings that are relevant to highway operations and incident management.

l. Training Mode: The IIE system should have online training tools for training new users and for conducting simulated practice exercises.

3. Conceptual Configuration Design Requirements

The IIE system requirements identified in the Report on Table Top Sessions and Data Interoperability Requirements included several requirements that impact the conceptual design of the system. These requirements are identified below, along with additional requirements appropriate to the deployment of a system of this type:

a. Redundancy: The role that the IIE system will play in public safety dictates that the system must be highly reliable and exhibit extremely high availability. High availability implies that servers, interfaces, and critical infrastructure must be redundant, and utilize high availability technologies such as fault-tolerant servers and/or hot-standby configurations.

b. Survivability: The IIE system must be able to survive any natural disaster and/or "attack" on its infrastructure. This survivability requirement implies that the redundant elements of the configuration be geographically separated and physically secured, so that critical functions continue to be available even if a disaster or terrorist attack destroys or severely impacts a critical site.

c. Security: The IIE system must be fully protected from all forms of Cyber attack, including unauthorized access, viruses, worms, and denial of service attacks that could overload the IIE system resources. The IIE system must employ secure password and authentication measures to protect against unauthorized access. Interfaces to Public Safety CAD systems must protect the integrity of those systems, the secrecy of law enforcement operations, and the privacy of the general public. All data transmissions across the infrastructure, whether over wireless or terrestrial transmission facilities, should be encrypted. Secure tunneling protocols, such as VPN (Virtual Private Network) should be employed to provide a secure connection between the end user and the IIE system servers. The IIE system should maintain an audit trail of all user logins, actions, and entries to aid in the investigation of any security breaches.

d. Accessibility: The IIE system must be accessible to any authorized user from any fixed or mobile location and from any type of modern computing device.

e. Scalability: The IIE system should be scalable to support an expanding base of participating agencies and users. It should be possible to support a gradual rollout of the IIE system on a regional or corridor basis by initially deploying a subset of the resources and infrastructure that will be needed for the ultimate deployment across the state, and to gradually expand these system resources as they are needed. In addition to this planned scalability, the IIE system should be expandable to support unanticipated growth in functionality and user participation.

f. Shared Use of Communications Infrastructure: Deployment of a dedicated state-wide terrestrial and wireless data infrastructure, solely for the use of the IIE system, cannot be cost justified. Data interoperability between Public Safety and transportation agencies is just one aspect of the data communications that occur within these agencies; the vast majority of data communications volume within these agencies is to support each agency's specific mission critical functions. These agencies, alone and in cooperation with neighboring agencies, have developed and largely justified wireless mobile data and "backbone" infrastructures to support these internal operational needs. The IIE system data communications must be able to take advantage of, and utilize, these existing and future agency infrastructures as well as other, more-public communications infrastructures, such as the Internet or those of commercial wireless service providers. Such shared use of multiple infrastructures implies that the IIE system communication protocols be routable and that data communications be highly secured by the use of end-to-end encryption.

g. Roaming: Users should not be constrained to a specific geographic area to utilize the IIE system. Users should be able to access the IIE system when they are roaming outside of their home territory, such as when public safety personnel are responding to mutual aid situations.

h. Independent of Communications Infrastructure: The IIE system should be accessible to users from dispatch and operations centers, offices, vehicles, and home. To meet this requirement, the system must be accessible via a broad range and combination of public and private, terrestrial and wireless infrastructures. These infrastructures include:

- Internet, via dialup, DSL, Cable TV, and wide-band ISP connections
- BadgerNet
- Private Public Safety Wireless Mobile Data systems, including the State Patrol's statewide mobile data system
- WisDOT Touch America fiber network
- State Patrol statewide digital microwave radio system
- Cellular network wireless data services
- Wireless "hot spots".

i. Support multiple different connection speeds/bandwidth: The IIE system must be sensitive to a user's connection speed. This requirement is most applicable to graphical data, such as video, pictures, and maps. For example, video sent to users with low speed connections should be reduced in resolution and/or frame rates. In some cases, such as low speed wireless mobile data networks, the transfer of high bandwidth data, such as video, should be prohibited so as not to overload the network and impact the response time of critical law enforcement applications.

j. Support for Multiple Wireless Mobile Data infrastructures: Many Public Safety mobile data systems currently in use in Wisconsin are closed systems and utilize proprietary protocols and therefore will not readily be able to interface to the IIE system. In some cases, these systems can easily be modified to provide the desired connectivity. In other cases, modification will not be cost effective. For these systems, participation in the IIE system may have to be deferred until the existing mobile data system is replaced. Alternatively, the routing capabilities of mobile data computers can be used to route IIE system applications over a cellular data service.

k. End User Computing Devices: The IIE system should support a complete range of modern computing devices for data input and display, including Public Safety CAD terminals, personal computers, mobile data computers, PDAs, and cell phones equipped with PDA capabilities. For alerts and text message exchanges, the IIE system should also support devices such as dedicated email devices (BlackBerry), text pagers, and the short text messaging (SMS) capabilities of cell phones.

l. Interfaces: To provide the desired information, and to minimize the duplication of data entry, the IIE system will need to interface to numerous systems across the state, including:

1. Public Safety CAD Systems, including the State Patrol CAD System
2. State Patrol Wireless Mobile Data System
3. Public Safety Wireless Mobile Data Systems
4. Traffic Management Systems
    - MONITOR
    - CCTV Video Systems
    - Road Weather Information System
5. EPAD
6. Data Archiving System
7. Internet, both for connectivity and for access to Public Safety information, such as Hazmat data.
8. Future Interfaces
    - 511 System (possibly CARS)
    - Emergency Management Crisis Information Systems

m. Operations and Maintenance: The IIE System must be easily managed, updated, and maintained from a central location and by the agencies themselves. Ease of maintenance and system management implies that use of any IIE system-specific client software on

the user's end device should be minimized. This can best be achieved by employing Web Server/Browser based system architecture for the IIE system applications. This architecture places minimum requirements on the end user device. Typically a standard Internet browser will be the only application necessary on the end user device.

n. Use of Standards: The IIE system should make maximum use of the standards that have been developed for data communications and incident management in the IT, ITS, Emergency Management, and Law Enforcement industries. Because CAD and mobile data systems are procured independently by each agency, these standards should be field proven, fully defined, and testable in the factory, prior to deployment in the field.

o. Use of Off-the-Shelf Components: The IIE system should make maximum use of commercial off the shelf (COTS) hardware and software.

p. Supplement Existing Systems: The IIE system must be able to co-exist and share infrastructure with other agency systems. Agencies have invested significant resources in these systems, and have developed applications that address their specific needs. Work processes have evolved to fully incorporate the use of these systems. The objective of the IIE system is not to replace these applications or require re-engineering of processes, but rather to augment these applications with new applications designed to share information among agencies, in a manner that complements the existing workflows.

q. Compliant with ITS Architecture: The IIE system must conform to the plans, data structures, and information exchange standards dictated by the State, Regional, and National ITS Architectures.

4. System Design Resources

An early phase of the Traffic Operations and Public Safety Communications Interoperability Assessment & Plan project was to conduct interviews with stakeholders around the state to identify existing interoperability programs and state-wide communications infrastructures that could be employed for meeting the data interoperability objectives. Seven infrastructures were identified during these interviews as potentially useful in implementing the IIE System:

- WisDOT Touch America fiber
- State Patrol Digital Microwave Radio System
- State Patrol Wireless Mobile Data System
- WIJIS system
- Badgernet
- Commercial Wireless Service Providers
- Commercial Internet

An overview description of each of these infrastructures is provided in the following sections.

4.1 WisDOT - Touch America Fiber

The WisDOT fiber optic communications network along I-94 was initially facilitated by an agreement with Touch America and has been enhanced by subsequent agreements with other organizations. The fiber was originally intended for WisDOT traffic and incident management use; however its use continues to expand both in application and volume. Video exchange with State Patrol Districts and local police, and data communication between TOCs, and between TOC and 911 Communication Centers, have been implemented. Future considerations include a storage area network and backup communications for a portion of the State Patrol microwave.

4.1.1 Route

In general, the fiber follows I-94 from Illinois to Minnesota. Loops have been established in the cities of Milwaukee, Waukesha, and Madison. In Watertown, the route diverts from I-94 for a distance of about 12 miles.

Expansion of the fiber communications from Milwaukee to Green Bay to Chippewa Falls, and from Madison to Fond du Lac, which would add two more loops to the network, is under consideration.

4.1.2 Configuration

WisDOT has its own 36-strand, single-mode fiber cable and conduit, which was buried at the same time as the Touch America fiber. Allocation of the strands is as follows:

- 12 are currently allocated to each district for their own use
- 12 are currently being held in reserve
- 8 are leased to outside organizations (see below)
- 4 are used for the DOT backbone

The WisDOT backbone has the following attributes:

- SONET ring (ring is collapsed into the fiber cable; there is no divergent path except where loops are implemented)
- OC-48 capacity (2.5 Gbps), organized into 100 Mbps Ethernet ports
- Drop/add equipment at State Patrol Districts 1, 2, and 5, WisDOT District 1 Operations, and WisDOT District 2 TOC; additional drop/adds at State Patrol D6, DTD District 6, and Hill Farms by the end of 2004
- Node equipment has been standardized on Cisco model 15327 and 15454 series
- Node power from UPSs at State Patrol locations, from 48Vdc battery (20 hr capacity) at other locations

- Monitoring and maintenance is externally contracted
- Regen equipment is installed at several locations along the right-of-way.

4.1.3 Agreements/Financing

The primary agreement with Touch America provides usage (not ownership) of the fiber until 2040 in exchange for right-of-way access along the I-94 corridor. Additional parties were involved in the agreement for the interconnection with MinnDOT over the St. Croix bridge.

Other agreements that provide supplementary funding and/or access rights include:

- Fiber usage was exchanged with the Department of Corrections to obtain fiber to the Hill Farms complex.
- University of Wisconsin leases four dark fibers from border to border, along with facility space, for communication with other universities.
- The Wisconsin National Guard leases four dark fibers and facility space between Madison and Fort McCoy.

4.2 WSP - Microwave Radio System

The Wisconsin State Patrol's (WSP) microwave radio system is managed by the WSP's Bureau of Communications (BOC). It is deployed over a considerable portion of the state supporting the voice and data two-way radio communications needs of several state agencies. Late in 2003, the BOC completed an upgrade to the system that consisted of the following:

- Conversion to full digital operation.
- Addition of new path segments.
- Rerouting of certain path segments.

4.2.1 Route/Configuration

The system is currently comprised of approximately seventy-four (74) antenna sites of which approximately thirty (30) form the basis for its dual-loop topology design. One of the loops serves the eastern half and the other one serves the western half of the state. Both loops share common path segments in the central part of the state.

The topology is also characterized by a number of branch segments emanating from the loop sites that served other antenna sites including those serving the State Patrol District Offices and the Police Academy. In all, the system has a presence in fifty-five (55) of the seventy-two (72) counties in the state.

The entire loop and some of the branch segments, collectively the primary, operate in the licensed 6 GHz band while other branches operate in the unlicensed 2.4 and 5.8 GHz bands. DS-3 (28T1) capacity is available on all the system's loop path segments in addition to those branch segments serving the WSP District Offices. The remaining branches currently offer significantly reduced capacity.

4.2.2 Future Expansion Plans

Expansion of the primary segments of the system to OC-3 (84T1) capacity is currently being contemplated, however, no tangible plan or funding for such expansion exists today. This expansion would increase the system's current capacity on these primary segments by a factor of three (3).

4.3 State Patrol Wireless Mobile Data System

The State Patrol Wireless Mobile Data System, commonly referred to as the MDCN (Mobile Data Communications Network), is used by approximately 144 organizations throughout Wisconsin. These organizations, engaged mostly in law enforcement, are currently comprised of 6-state, 29-county, 104-local, 2-tribal and 3-federal agencies. There are approximately 1,300 mobile computer terminals (MCT) on the system, and approximately 350 MCTs are typically logged in at any one time. The State Patrol and the Department of Natural Resources account for slightly more than half of the MCTs on the system today.

4.3.1 Existing System

The existing system is based on IPMobileNet's family of wireless fixed access points and mobile radio modem products. It operates at an over-the-air (OTA) data communications speed of 4,800 bits-per-seconds using a proprietary, contention-based protocol. Each MCT has a serial connection to a vehicular-mounted IPMobilenet radio modem. Middleware in the MCT makes the data network transparent and provides the appearance of an IP network to MCT software. Data transmission security is achieved via a combination of encryption, compression, and the proprietary protocol.

The state is divided into seven (7) MDCN regions with each one supported by multiple radio antenna sites. Approximately seventy-two (72) antenna sites currently comprise the system providing radio coverage over roughly 90% of the state. Each region uses a single, paired-frequency radio channel in the 140 MHz military band. A statewide pool of four (4) MDCN radio channels is shared amongst the regions. The State Patrol is trying to acquire additional channels in the VHF (150-160 MHz) radio spectrum to replace these military frequencies, most of which must be relinquished by 2008 (all by 2010); and to meet future demands for growth.

When an MCT transmits, several towers in the region may pick up the signal. All such received signals from each tower in a district are brought back to the district, consolidated using a channel bank, and sent over the State Patrol microwave system to the radio network controller in District 1. The radio network controller determines which tower to use to send the response. As an MCT travels between regions, loss of its home region channel will cause the unit to automatically search for a new MDCN channel; this functionality provides the users with a truly statewide system.

The radio network controller is connected to a server operating as a message-switching type device that provides connectivity to the State Patrol's Computer Assisted Dispatch (CAD) system, to the DOJ databases, and to the ETIME system. Access is provided to State and Federal law enforcement

records (wants/warrants, criminal history, motor vehicle information), information/alerts, text messaging, unit status, emergency alarms, and applications used by motor vehicle inspectors. The CAD interface is used primarily for text messaging and reporting unit status. The system does not currently support automatic vehicle location (AVL) functionality or the CAD systems of other participating agencies.

State Patrol operates and maintains the fixed-end equipment (including, base stations, towers, microwave backbone, and message switch). Member agencies purchase their own vehicle equipment but otherwise bear no costs for using the network. State Patrol provides technical phone support for the smaller agencies, which is quite time consuming. The system has a VPN channel to the vendor's factory for maintenance support. The MCT client software, middleware, radio network controller, and message switch were provided by HTE.

4.3.2 New System

State Patrol is converting to a new IP-based mobile data system that operates at an over the air data communications speed of 19,200 bits-per-second, four times the speed of the existing system. The most significant advantage of this new system is that it will be able to support true end-to-end IP connectivity. The MCT Ethernet port connects directly to an IPMobilenet radio modem and a TCP/IP socket is used to communicate via IP to the message switch; no middleware is required.

The new IP-based controller is a pair of fault tolerant Linux servers. Currently both servers are located at District 1, however, one is planned to be relocated to an off-site facility to enhance system survivability. Failover, which is accomplished by swapping IP addresses, takes approximately 45 minutes and may cause temporary disruption of existing operations during the swap. The new system uses different frequencies in the 150-160 MHz band, but will initially still use one frequency per tower site as the existing system does today. A second channel can be added, if available, and the IP controller will automatically balance the load on both channels to maximize data throughput efficiency. The MCT's will monitor quality of service in addition to signal strength to determine whether to switch to the roaming mode.

The old and new systems will operate in parallel during transition. State Patrol District 1 is now operational on the new system with 25 vehicles. Usage by other agencies will not be permitted until the State Patrol transition is complete.

The new system supports all the functions provided by the system it replaces. In addition, the new system will provide a direct interface to DOT vehicle/driver databases, direct transfer of data from motor carrier inspections, electronic time sheets, automated citations with electronic delivery to the circuit courts, "Green sheets", interface to the State Patrol CAD system, direct data communications dispatches to the MCT units, amber alerts, and low resolution photographs (both to the MCT, probably using a web page format, and from the MCT, for applications such as pictures of an accident). Most new functionality will likely utilize a web-based interface.

Both the MCTs and IPMobilenet radio modems have GPS receivers. Although no formal AVL tracking is currently being performed, State Patrol is conducting tests of an AVL application that polls vehicles for location information every few seconds and displays the locations on a map; if the tests are successful, the AVL package may be integrated into the existing HTE CAD system. Display of vehicle locations on a map on the MCT is also under consideration.

4.4 Wisconsin Justice Information Sharing Program (WIJIS)

The Wisconsin Justice Information Sharing Program (WIJIS) is a program authorized by the State of Wisconsin to facilitate justice information sharing among Wisconsin justice organizations. WIJIS is responsible for promoting and coordinating automated justice information systems that are compatible among, and available to, local, county and state agencies.

WIJIS integrators plan to develop a secure Justice Web Service that will allow county and state agencies to share local information assets while retaining existing information systems.

WIJIS activities include:

- A proposed demonstration project to develop a secure web service for the creation of an inter-county query between disparate District Attorney case management systems and the development of read-only access to these systems for law enforcement agencies. The demonstration project will serve as a test bed for evaluating a statewide web service approach and the security architecture necessary to protect it.

- Organizing an inter-agency workgroup to share information, to work on inter-agency projects and to represent the interests of the Wisconsin Departments of Justice, Transportation, Electronic Government, the Office of Justice Assistance, State Public Defenders Office, Wisconsin Supreme Court, local law enforcement agencies, etc.

- The identification of other non-web service solutions that would achieve the state's goals to enable information sharing among the state's justice partners.

- Providing guidelines and advice concerning non-technical or system matters such as the type of agreements that are required among agencies in order to build an enterprise-wide information sharing system.

4.5 BadgerNet

BadgerNet, the official State of Wisconsin information system, is accessible to Public Safety agencies, school districts, the Department of Justice (DOJ), state private colleges, and some cities in Wisconsin. There are currently 1,800 connection points to BadgerNet even though access is limited to public and not-for-profit agencies.

The State of Wisconsin leases fiber for Badgernet through Norlite Communications. The fiber communications (SONET) operate at OC-3 (155 Mbps).

With the authorization of the WIJIS (Wisconsin Justice Information Sharing) program by the State of Wisconsin, a means of intercommunications is needed to support information exchange among systems used by the numerous and disparate organizations involved in law enforcement, court operations, administration, district attorneys and attorneys general, public and private defenders, corrections, etc. Most of these systems already have access to BadgerNet, making BadgerNet an important component of WIJIS. Most systems that do not have access to BadgerNet do have access to the Internet, allowing the Internet to supplement BadgerNet in bringing WIJIS to additional agencies (security and authentication is required whether an agency uses BadgerNet or the internet for WIJIS functions).

Funding for Badgernet is obtained through the Wisconsin Department of Administration (DOA).

4.6 Commercial Wireless Service Providers

There are several commercial wireless service providers (CWSP) today offering wide area coverage radio systems that support the wireless transmission of data between fixed locations and roaming or fixed field devices. These public-use cellular-type architecture systems are available to any subscriber desiring to lease "air-time" to send and receive data wirelessly. These systems include specialized mobile radio (SMR) and enhanced specialized mobile radio (ESMR) operators, and cellular telephone companies.

These wireless infrastructures are a shared access "public" network that is leased to a multitude of users for day-to-day business or, simply, for personal use. Users are responsible for the outlay of capital expenses for their field equipment (mobile or vehicular radio devices), all other expenses associated with the interconnectivity to the CWSP, and the recurring expenses associated related to the use of the infrastructure.

CWSPs use wireless infrastructures that are comprised of radio antenna sites and frequencies that are owned, operated and maintained by the CWSP. These systems are characterized by their corporate charters to serve the general public and maximize their revenue; and are, therefore, most interested in adding as many users as possible on their systems. In addition, users have no control over the system's design, redundancy, operations, or maintenance.

On heavy subscriber-loaded systems, access delays during busy usage periods[1] can be excessive and there is virtually no guarantee of access, even for Public Safety organizations.[2] For this reason, these types of systems are not well suited for supporting mission-critical or time-sensitive data

[1] While these periods generally occur during the daylight business hours, they are also influenced by large scale weather or emergency related events.
[2] Since the events of September 11, 2001, some CWSPs have begun to offer service level contracts for network priority access to public safety first responders. Nextel is one of these CWSPs.

communications. Despite this, however, public systems can complement a private radio system under certain circumstances. An example of this would be to relieve channel congestion on a privately-owned system, such as the WSP's mobile data communications network (MDCN), by relocating non-essential communications to a CWSP.

In Wisconsin there are several major CSPs, these are:

- AT&T Wireless
- Cingular Wireless
- Nextel
- Sprint PCS
- T-Mobile
- Verizon Wireless
- US Cellular

There are also others that can be classified as minor CSPs, these were identified as:

- Monet Mobile
- Motient

One of the distinctions between a major and a minor CSP is the geographical area of service they offer. Major CSP's in Wisconsin provide service over significant portions of the state choosing to concentrate primarily in populated urban and suburban areas and along well-traveled highway corridors. On the other hand, minor carriers offer service in only a few select areas of the state.

Another distinction between major and minor CSP is in the type of wireless service they offer. Major CSPs offer wireless data as on overlay to their core cellular telephone service, in effect providing an infrastructure that shares both voice and data communications. Both of the minor CSPs identified herein having taking a more focused approach by offering wireless data service exclusively.

The most striking difference between these commercially available networks and privately owned infrastructures is in two areas. They are:

- Implementation. With a privately owned solution, the owner must deploy a wireless infrastructure. With a leased commercial solution, the wireless infrastructure is already in place. This lends itself to very quick implementations of user applications.

- Monthly Recurring Expenses. The leased commercial solutions will require payment of a monthly fee per subscriber. Fee structures are based on measured usage or on unlimited use, and on length-of-service commitments. The choice of a measured usage solution must be evaluated carefully as exceeding the basic usage allowed can be expensive.

It must be re-emphasized that these networks are public and, therefore, the subscribers have very little control over the data traffic on the network. In this type of environment, some users can occupy a substantial portion of the network forcing other users to endure less than optimum performance. Although the networks are designed to keep users from continuously occupying the network for extended periods of time, there is always the risk that users may experience, from time to time, delays in gaining access to the network.

The capacity of these networks is contingent on the number of radio frequencies the network operator provides over the desired service area. The greater the number of frequencies available the greater the number of subscribers supported, and the better the network's performance will be. Customarily, the network operators hold the information on the number of frequencies in a given area confidential, however, they are usually more willing to share this information in response to formal procurement solicitations or when engaged in direct negotiations with potential subscribers.

Typically, the service providers are proactive about maintaining acceptable levels of performance. For example, this could be achieved by the service provider having an operation control center as part of their network's architecture. However, it is always advisable to pursue network performance requirements and non-performance penalties as part of a service agreement.

Another important aspect when considering the services of a leased commercial service is that of network expansion for either increasing coverage, increasing capacity performance, or for satisfying unique user coverage requirements within the existing coverage area. While operators can easily achieved this by increasing the number of antenna sites or by adding frequencies, their commitment to expansion should be addressed prior to finalizing a service agreement.

5. Technology Trends

Due to budgetary constraints and heavy dependence on the evolution of state-wide infrastructure, a long planning horizon (+10) years has been established for ultimate statewide deployment of the IIE system, with possibly some limited initial deployment beginning within the next 3-5 years. With deployment of the system occurring several years in the future, the conceptual design should not be overly constrained by existing technologies and infrastructure. More appropriately, the conceptual design should be based on technology and infrastructure advancements that are likely to be in place several years from now. The following sections discuss these technology trends along with other trends that are relevant to the conceptual design.

5.1 Wireless Mobile Data

The ability to work away from the "traditional" office environment and remain "connected" is a need that has been identified by the mobile workforce for some time. Wireless communications systems have emerged as a powerful work tool that allows organizations to manage their field resources in order to maximize the effective and efficient delivery of the services they provide.

In recent years, advances in wireless communications technologies have made it possible for data applications, historically limited to cable or wired environments, to be used "over-the-air." Additionally, the introduction of wirelessly-enabled laptop computers and other types handheld devices is making the mobile workforce's need for untethered portability a reality.

Many existing privately owned mobile data systems have very limited opportunities for application growth as compared to those emerging technology platforms offered by leased commercial networks. This has been due primarily to the proprietary nature of these privately owned systems. However, with the emergence and the non-proprietary nature of some of these new technologies, computer applications limited to the traditional wired networks (LANs and WANs) will be possible through a wireless environment.

The following sections highlight some of the trends in wireless mobile data.

5.1.1 700 MHz Spectrum

In 1996, the FCC commissioned a study to investigate the current and future two-way radio communications needs of state and local public safety/service agencies and make recommendations to ensure that adequate radio frequency spectrum is made available to those agencies. One of the key findings of the study was that the existing radio spectrum allocations are insufficient to meet the current and future communications demands for voice, data, and imaging.

In response to the recommendations of the study, the FCC reallocated spectrum in the 700 MHz band to these agencies. Each channel in the band has a 50 KHz bandwidth, which under current technology will support data rates of up to128 Kbps. The FCC will also allow licensees to aggregate up to three 50 KHz channels, for a total bandwidth of 150 KHz with the capability to support data rates of 384 Kbps on the aggregated channel.

The 700 MHz band allocated by the FCC to Public Safety use is currently used by television broadcasters and represents the spectrum comprised of UHF-TV channels 60 through 69. The date December 31, 2006 was established as the milestone by which TV broadcasters are to vacate the reallocated spectrum provided they meet certain viewership criteria. There is currently widespread speculation that incumbent TV broadcasters will not be able to vacate this spectrum by December of 2006. Additionally, the public safety/service community is concerned that unless a firm cutoff date is established, devoid of viewership criteria, the much needed spectrum will not be easily relinquished by the TV broadcasters. The FCC is currently considering a new cutoff date of December 31, 2008.

In the state of Wisconsin, the entire southeastern portion of the state is affected by incumbent TV broadcasters. This area represents roughly 1/3 of the state. Therefore, the availability of 700 MHz band use by the State within this area is very unlikely in the short- to medium-term.

5.1.2 Wireless Metropolitan Area Networks.

Wireless Metropolitan Area Networks (WMANs) use the recently developed IEEE 802.16 standard, commonly referred in the industry as WiMAX. It is intended to cover distances greater than those of typical 802.11 WiFi "hot-spots" and its use is best described as technology that supports fixed point-to-fixed point or fixed point-to-multipoint data transmission applications. It is being touted as the wireless solution for the "last mile problem" as it can be an alternative for cable, DSL or fiber optic service.

WiMAX uses more sophisticated data transmission protocols than 802.11, which result in improved connectivity, reliability and quality of service. Because it uses fairly broad radio frequency bandwidth (typically 10 MHz) it can support high-speed, low-latency data communications for applications such as Internet access, voice-over-IP and motion video. It can also be used to aggregate WiFi networks and provide long distance backhaul to other core data communication networks.

A variant of WiMAX designated as the IEEE 802.16e (Mobile WiMAX) standard is currently under development. When completed this standard will be able to support roaming mobile devices with data transmission speeds approaching those of 802.16 at vehicular speeds in excess of 75 mph.

5.1.3 Local Area Network (802.11 WiFi)

Wireless Local Area Networks (WLANs) use several variants of the IEEE 802.11 standard. These variants operate in different unlicensed radio frequency bands supporting the following over-the-air (OTA) data communication speeds:

- 802.11a supports OTA of up to 54 Mbps in the 5.8 GHz band
- 802.11b supports OTA of up to 11 Mbps in the 2.4 GHz band
- 802.11g supports OTA of up to 54 Mbps in the 2.4 GHz band

These standards use low radio frequency power (typically 600 milliwatts) allowing for a wireless coverage range of about 300 feet. They are predominantly found in "hot spots," such as cafes, hotels, airports, offices and home networks. These three versions of the 802.11 standard are commonly used and built into most modern laptops and mobile devices.

Wireless local area network (WLAN) technology is currently being used by organizations as an alternative or supplement to low speed wireless connections for sending and/or receiving large data files that are not realtime critical. Private WLAN's provide a close proximity wireless connection to established terrestrial based LAN's and WAN's.

This technology is not well suited for wide area wireless communications due to the large number of radio antenna sites required. However, it can be economically deployed to cover smaller areas such as the inside of buildings, exterior areas of buildings in complexes or campuses, or as roadside access points for mobile users.

5.1.4 Mesh Networks

Mesh-network technology extends the range of traditional WLANs by allowing a collection of 802.11 standard "nodes" (an individual laptop or fixed access point such as a hot spot) to interconnect and move data between nodes acting as one "shared" network. In a mesh network (sometimes referred to as "multi-hop" network) small nodes are installed throughout a large area, such as a neighborhood or school, and each acts as a router, transmitting data from one node to the next.

One advantage of mesh networks is the use of dynamic path configuration that allows RF signals to navigate around large obstacles, such as mountains or buildings. If one path to the base station is blocked, a transmission using a mesh network will automatically find another path through another node. Another advantage is reliability. In a "single-hop" network, if one node goes down, the entire WiFi LAN network goes down. In a mesh-network architecture, if one node goes down, the network continues to operate by routing data through other nodes.

5.1.5 Personal Area Networks

Wireless Personal Area Networks (WPANs) use two type of standards: the IEEE 802.15.1, commonly referred as "Bluetooth," supports over-the-air (OTA) data communication speeds of up to 1 Mbps; and the IEEE 802.15.3 or Ultra-Wide Band (UWB) standard supporting OTA speeds of over 400 Mbps. Both utilize very low radio frequency power (typically 1 milliwatt) allowing for a very short wireless coverage range of about 30 feet. They operate in the 2.4 GHz unlicensed frequency band, which is also the same band used by 802.11 WiFi type networks. These standards were specifically developed for supporting very small networks within a confined place, such as home office, desk or inside a vehicle.

Bluetooth is intended to be used primarily for wirelessly interconnecting computer or communication peripherals, such as personal computers, radio modems, GPS location receivers, printers, personal digital assistants, cellular phones, etc. A recent application of this technology is in cellular telephony where a wireless headset can now provide an un-tethered interconnection to a belt-worn cellular telephone. Bluetooth enabled products are starting to enter the marketplace in greater numbers.

UWB provides greater over-the-air data communications speed than Bluetooth. This makes it ideal for heavy data-payload multimedia-type applications, such as DVD-quality video to shared wirelessly in a home or small office environment.

5.1.6 Satellite

This technology is based on low earth orbit satellites (LEOS) providing the wireless connectivity to mobile data units. These LEOS are in geostationary orbit usually between 400 to 600 miles above the earth's surface and operate at frequencies greater than 1,300 MHz. In some cases, this service is being used to augment a user's terrestrial based system. One of the attributes of these systems is their ability to provide near seamless wireless coverage over the user's entire service area without the need for deploying multiple terrestrial radio antenna sites.

Satellite systems communicate at very low data communication speeds as compared to traditional satellite based services and other terrestrial based wireless technologies. Typical data transmission rates are between 2,400 and 6,700 bits-per-second. This service is also capable of supporting voice communications. Satellite communications are known to experience delays not found in terrestrial based systems. This is mainly attributed to the fact that all satellite users must share the communications channels available on the satellite.

Satellite mobile data technology was developed primarily for mobile (as opposed to handheld) use to meet the very wide area or national wireless coverage requirements of trucking and railroad companies. One of the attributes of these systems is their ability to provide near seamless wireless coverage over the user's entire service area without the need for deploying multiple terrestrial radio antenna sites. However, recently it has gained popularity by meeting the small regional coverage requirements of utility, transportation, and other service related companies.

In public safety, Macro is aware of one statewide law enforcement agency that has been experimenting with this technology. Because of the state's extremely mountainous terrain, this technology promises to provide a more economical solution over a traditional terrestrial based system. In this case, capital costs associated with the deployment of a user-owned infrastructure would be virtually non-existing.

Because of their high frequency of operation, these systems will generally require an unobstructed signal path between the mobile unit's antenna and the overhead satellite. Places such as tunnels, highway under-passes, covered parking garages, etc., are locations in which reliable communications will be greatly reduced or will not be possible. On the other hand, terrestrial based systems are less susceptible to obstructed signal paths.

Current recurring subscriber use rates for this type of service are greater than those of commercial-based terrestrial systems. Fees charged are based on the monthly amount of data sent or received by each mobile unit rather than based on unlimited usage plans typically offered by terrestrial service providers. Data usage exceeding rate plan thresholds are almost always charge at a significantly greater rate than that of the rate plans.

Satellite service data transmission rates are very low as compared to those available from terrestrial based systems. At least in the short term, there seems to be very little interest from the satellite providers to provide the same level of service as those of the terrestrial based systems. Without a significant improvement to their data rate offerings and service pricing it is highly likely that this type of service will continue to remain the solution of only a few users. For the State's area of operation, terrestrial based leased systems can provide wireless coverage equal to or better than that provided by satellite and at significantly less cost. In summary, it is our opinion that satellite wireless data services fall short of the benefits provided by terrestrial based systems. Therefore, this wireless data solution is not a desirable technology for the State to deploy.

5.1.7 Mobile Computer Support for Multiple Radios

Over the last several years, the emergence of privately owned, commercially leased, and short-range, high-speed wireless data technologies has created a mobile data environment that offers a choice of several system solutions to meet different user needs. However, in certain situations, it has become apparent that a single wireless system solution has not been able to satisfy all of a user's wireless data needs effectively.

Multi-system gateways and applications enable properly equipped mobile devices to seamlessly roam between different wireless systems. These products perform automatic selection of the wireless systems based on user-configurable parameters, or existing system or field conditions, allowing mobile data users to transmit and receive data in the most effective and efficient manner. Several manufactures currently offer these types of products.

5.2 Other Trends

In addition to the trends in wireless data technology described in the sections above, the conceptual design of the IIE system should recognize and take advantage of the following technology trends:

a. Internet Speeds and Access: The trend in terrestrial and satellite commercial communications infrastructure and Internet Service Providers (ISPs) is to make higher speed access to the Internet more widely available at decreasing costs. This trend will not only make high-speed Internet readily accessible and cost-effective for almost all agencies, but will eventually bring this capability to most private residences. High bandwidth Internet capabilities will be needed to access map-based IIE System applications and video. For agencies located far from WisDOT's Touch America fiber, high speed Internet may be the only possible means to access real-time or near full-motion video.

b. Internet Security: Internet security is already a critical concern in the commercial world. The Internet is being used more and more for mission critical business and financial transactions. Technologies are constantly being improved for protecting such data, as well as the target systems that utilize this data. One example of secure Internet technology that is currently employed is Virtual Private Network (VPN). VPN is a technology that establishes a secure "tunnel" to connect two points across a shared public network. Data sent across the shared network is encrypted and is "invisible" to other users on the shared network. VPN technology is widely available for network and end user devices. The trend in the industry will be for continued improvement in VPN-type and other security technologies.

c. Operating System Security: Microsoft Windows operating systems have been widely criticized for security holes that can be exploited by viruses and worms. Microsoft continually tries to plug these holes with security updates to their operating system. Microsoft's new operating system, code named Longhorn, is due for initial release in 2006. This operating system is reportedly being designed from the ground up with a high priority on security. The long-term trend in operating system development will be continued emphasis on security improvements.

d. Use of Secure Internet Technologies by Law Enforcement: Law Enforcement has understandably been extremely reluctant to open their law enforcement systems to the Internet. This reluctance stems from their legal responsibility to protect criminal data as well as their desire to protect officers and information associated with ongoing investigations. As Internet security technology improves, there has been some reduction in resistance to use such technologies. The best example is in the use of public wireless infrastructures and secure Internet technologies, to provide mobile data access to agency and state crime databases and applications (connections between the mobile data switch and crime database centers, however, must still typically be dedicated point-to-point connections that do not share any other data applications). Another example is the Wisconsin Justice Information Sharing program (WIJIS) initiative to develop a "Justice Gateway" and web services to provide access via secure Internet, and other means, to crime data stored on Law Enforcement Agency Records Management Systems (RMS) throughout the State of Wisconsin. With improvements in Internet security, and the emphasis of Homeland Security on the sharing of information between agencies, the trend will be for expanded acceptance and use of secure Internet technologies by Public Safety agencies.

e. WisDOT Touch America Fiber: As discussed in Section 2.3.1 above, WisDOT is currently in discussions to expand it's state-wide fiber resources north to Green Bay and west from Green Bay to Eau Claire, which when combined with WisDOT's I94 Touch America fiber network would form a large fiber loop, bringing high-speed access to WisDOT traffic systems and video much closer to additional WisDOT and State Patrol districts, as well as 911 communication and dispatch centers.

f. State Patrol Microwave Network Bandwidth: As mentioned earlier in this report, the existing WSP digital microwave radio system currently supports DS-3 (28T1s) capacity over most of the system and there is a desire to expand to OC-3 (84T1s) capacity at some future date. Once OC-3 is implemented, the system will have reached its upper limit of capacity. Expansion beyond OC-3 will require deployment of another microwave radio system layer. While microwave radio does not generally support the capacity available through fiber optics (OC-48 or 1,344 T1s in the case of the Touch-America fiber), it offers a resource that is flexible and easily deployable when compared to the deployment

of a fiber solution. This makes it an ideal resource for supporting locations that are not easily accessible with fiber or telephone company-leased data circuits.

g. CIMS Software: Crisis Information Management Software (CIMS) is a relatively new industry consisting of software systems and services to support Emergency Management operations. These systems tend to be Internet/web-based products with many CIMS providers also offering a service to host the software on their own servers (Application Service Provider (ASP) model). These products are available "off the shelf" with many of the same functions that have been identified for the IIE system. Common functions include browser-based user interface, map-based incident management, alerts, contacts, resource management, preplanned responses, reference data, training simulator, and electronic communications. The trend in this industry will be towards more standardization of functionality and interfaces. A product such as this can be used, for example, to seed a pilot project to test the benefits of a IIE system, before making major investments in infrastructure and custom software. The downside to these products is they have not been developed with highway operations in mind, so they do not conform to ITS data structure and interface standards.

6. Conceptual Design

The conceptual design presented in this report is intended to illustrate various key characteristics of the IIE System hardware and software configuration and infrastructure. The conceptual design shows how the requirements for functionality, availability, redundancy, survivability, security, scalability, connectivity, maintainability, and performance could be achieved in a conceptual framework. It is not the intent of this conceptual design to overly restrict future design and implementation phases. Deviations from this conceptual design should be considered, particularly if costs or risk can be reduced, provided that the required functionality, performance, and configuration characteristics are retained.

6.1 Data Interoperability Alternatives

In the voice world, interoperability focuses on the ability to conduct a voice conversation between members of different organizations across some communications medium. Solutions to voice mobile radio interoperability, for example, include putting all users on the same mobile radio system, establishing a bridge between disparate mobile radio systems, or using a third common radio system (e.g., mutual aid channels). In the voice interoperability world, the application, human speech, is taken for granted, because it already exists at both ends and the protocol has been standardized (e.g., English).

For interoperability to exist in the data world, three conditions must be satisfied:

1. There must be a physical communications path connecting the computer systems together. This can be a combination of dedicated and shared, landline and wireless links.

2. The systems must utilize a common data communications protocol(s).

3. Applications must be present that can interpret and process the data into useful information for the users.

A viable solution to many data interoperability problems is to agree on the data to exchange, agree on a format for that data, agree on a communication protocol, and establish a physical connection path. Each agency then independently decides what it wants to do with the data and develops its own applications. For the WisDOT Traffic Operations and Public Safety data interoperability study, this data-centric perspective is impractical. Literally hundreds of Public Safety and Transportation agencies could become involved in the IIE System. If the IIE system functions merely as a data exchange hub, the cost for each agency to further develop it's own applications would be prohibitive.

In discussions and Table Top sessions conducted with potential IIE system participants across the state, it was discovered that there is a high degree of overlap among agencies when it comes to data interoperability needs between Public Safety and Transportation organizations. A common set of functions was identified that meets the vast majority of these data interoperability needs. This study recommends the centralization of these applications as an integral component of the IIE system. Certainly a single development that provides the desired functionality is far more cost-effective than duplicating this development in each agency. The conceptual design, therefore, not only addresses the data exchange aspects of data interoperability, but also establishes the computer and software infrastructure necessary to deliver these applications to the IIE system participants.

6.2 Hardware Configuration

The conceptual design for the IIE system hardware configuration encompasses fixed and mobile users, mobile data infrastructure, landline and microwave infrastructure, system interfaces, and the computer configuration that provides the application functions identified in the requirements report. To illustrate these aspects of the conceptual design, three configuration diagrams are provided:

1. The IIE System Server Configuration Diagram (Figure 6.2-1) provides a conceptual design for the computer system necessary to link the end users and agency systems, and to provide the IIE system applications.

2. The CAD System Interface Diagram (Figure 6.2-2) provides a conceptual design for the interfacing of Public Safety CAD systems to the IIE system server farm. Included is an illustration of alternative methods for utilizing landline and microwave infrastructure to establish the physical connection between each CAD system and the IIE system. This diagram also shows how IIE system applications could be made accessible to Public Safety Dispatchers.

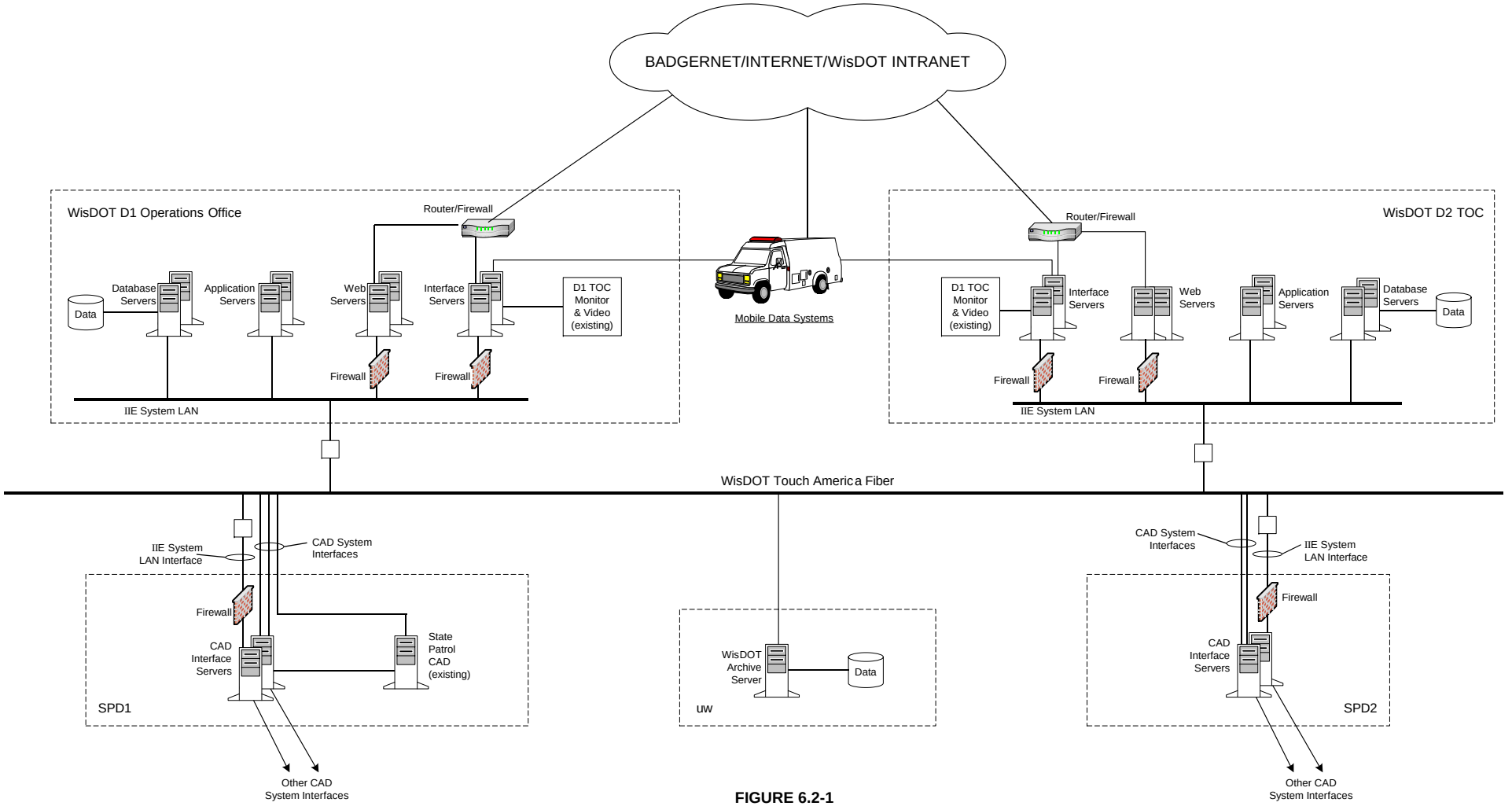

FIGURE 6.2-1
IIE SYSTEM SERVER CONFIGURATION

M:\WiSDOT\IIE System Server Config.vsd
02/16/05

3. The Mobile Data Conceptual Configuration (Figure 6.2-3) provides a conceptual design for interfacing mobile data systems to the IIE system server farm.

The IIE System conceptual design characteristics that are illustrated by each of these three configuration diagrams are described in further detail in the following sections.

6.2.1 Server Configuration

Figure 6.2-1 provides a conceptual design for the server configuration required to provide the IIE system interfaces and applications. Five different processing roles were identified as necessary to meet the IIE system requirements. These roles are represented as individual servers in the configuration diagram. The servers are segregated in this manner to illustrate different functional, redundancy/backup, and scalability requirements. In actual implementation, the role of a particular server may require multiple processors, or roles could be combined on a single processor, provided that each server role can be individually scalable to adapt to different growth rates as the system's use expands within the state.

The server roles, functions performed by each server type, and the redundancy and failover characteristics of each redundant pair of servers are presented in Table 6.2-1 below.

Table 6.2-1
IEE System Server
Conceptual Design

Server Role	Function	Redundancy/Failover Characteristics
Web Server	The web server(s) provides the user interface to the IIE system applications. The user interface will provide different display formats depending on the characteristics of the end user's computing device, and the bandwidth of the communications path. The web servers acquire their data from the application and database servers.	Web servers are shown as fully redundant for availability and disaster recovery purposes. In normal use, all available web servers could be employed to maximize the responsiveness of the system to user requests.
Application Server	The application server(s) hosts the software necessary to deliver the IIE System functions described in Section 2.2 above.	In general, one application server would provide the realtime functions and the second server would reside in a backup mode, ready to take over if the primary server fails.
Database Server	The database server(s) stores the realtime database, configuration data, and short-term historical data for retrieval by the application server.	Similar to application servers, one database server would service the realtime applications. Data should be replicated to the backup database server so that it could take over upon failure or loss of the primary database server.

Server Role	Function	Redundancy/Failover Characteristics
Interface Server	The interface server would provide the primary connection point for interfaces to Public Safety mobile data systems and the DOT traffic management systems.	Where possible, all interfaces to the IIE system should be redundant. One interface to a remote system (e.g., mobile data system or traffic management system) should terminate on one Interface Server, the second interface should terminate on the alternate Interface Server. Both Interface Servers should normally be on line. If a particular interface or it's communications path fails, only that interface should failover to the alternate Interface server. If an Interface Server fails, all interfaces should failover to the alternate Interface Server. This two- level redundancy will provide for a very high level of availability.
CAD Interface Server	The CAD Interface Server is a special version of the Interface Server. It is segregated from the general purpose Interface Server to meet the more stringent security requirements associated with protection of Public Safety CAD systems and crime data they contain. The CAD Interface servers should have no direct connection to the Internet.	The CAD Interface servers should employ the same two-level redundancy approach described above for the general purpose Interface Servers.

To protect against cyber attacks, and unintentional system corruption, IIE system servers that have connections to shared communications infrastructure, such as the Internet, or networked circuits on BadgerNet, should be protected by hardware or software firewall technology. Similarly, these servers should be isolated from the rest of the IIE system network by firewalls.

Redundant servers should be located in physically separate facilities to provide for disaster recovery. Preliminary recommendations for these sites, and the distribution of servers between sites, are shown on Figure 6.2-1. Site selection criteria included availability of local support staff, physical security, access to WisDOT Touch America fiber, and ease of interface to major external systems. It is stressed that these site recommendations are preliminary, as a detailed site survey/analysis is beyond the scope of this initial conceptual design.

The suggested sites for the Interface Servers, Web Servers, Application Servers, and Database Servers are the traffic management system equipment rooms at the WisDOT District 2 TOC and District 1 Operations office. These two sites offer direct access to the D1 and D2 traffic management systems (MONITOR System and video) and the support staffs for these systems. Both sites have access to WisDOT's Touch America fiber providing a high bandwidth connection for the communications among servers and the backing up of data. An alternative site in District 1 could be the computer rooms in the

WisDOT Hill Farms facility. This site would provide access to more IT staff than the District 1 location, but would have a less direct interface to the District 1 traffic management systems.

The suggested locations for the CAD Interface Servers are the State Patrol Headquarter facilities for State Patrol Districts 1 and 2. These locations have access to the WisDOT Touch America fiber, providing a high bandwidth connection with the other IIE System Servers. The server located at the District 1 Office will have direct access to the State Patrol CAD system and mobile data switch that are also located at the District 1 facility. By locating the CAD Interface Servers in the State Patrol offices other Law Enforcement agencies in the state can be assured that the CAD system interfaces are under Law Enforcement control and physical security. This should help overcome the natural reluctance of such agencies to resist opening up their CAD systems to any external system.

6.2.2 Public Safety CAD and User Interface

Figure 6.2-2 shows a typical configuration for the interfaces between a Public Safety Communication and Dispatch Center and the IIE system. Separate communication configurations will be required for a Public Safety CAD system interface to the IIE system and the IIE system user interface for dispatchers. These configurations are described in the following sections.

6.2.2.1 Public Safety CAD System Interface

The requirement to establish a link between an agency's CAD system and the IIE system is largely to eliminate any need for double entry by the dispatcher. Highway incident data is entered once on the CAD system, and is transferred to IIE system. If allowed by the agency, incident data entered into the IIE system by other agencies can flow back to the CAD system and enhance the CAD's system record of the incident. This approach allows the dispatcher to use the standard CAD incident screens for managing the highway incident.

It is recommended that the CAD system interface to the IIE system utilize point-to-point communication circuit connections and the IEEE 1512 communications protocol. The IEEE 1512 protocol is now being field tested in Seattle, Salt Lake City, and New York. This protocol was specifically developed for communications between Public Safety CAD systems and Traffic Management Systems and includes provisions to protect CAD system data. Only highway incident data would be "pushed" across the link. All other CAD incident types and data would be protected.

The agency's decision to implement a link between the CAD system and the IIE system will depend on the following factors:

- The ability of the CAD system to support a IEEE 1512 interface. Older CAD systems will likely not support this interface. If a major system upgrade is necessary to implement the interface, it may be more cost effective to defer implementation until the CAD system is replaced due to overall obsolescence.

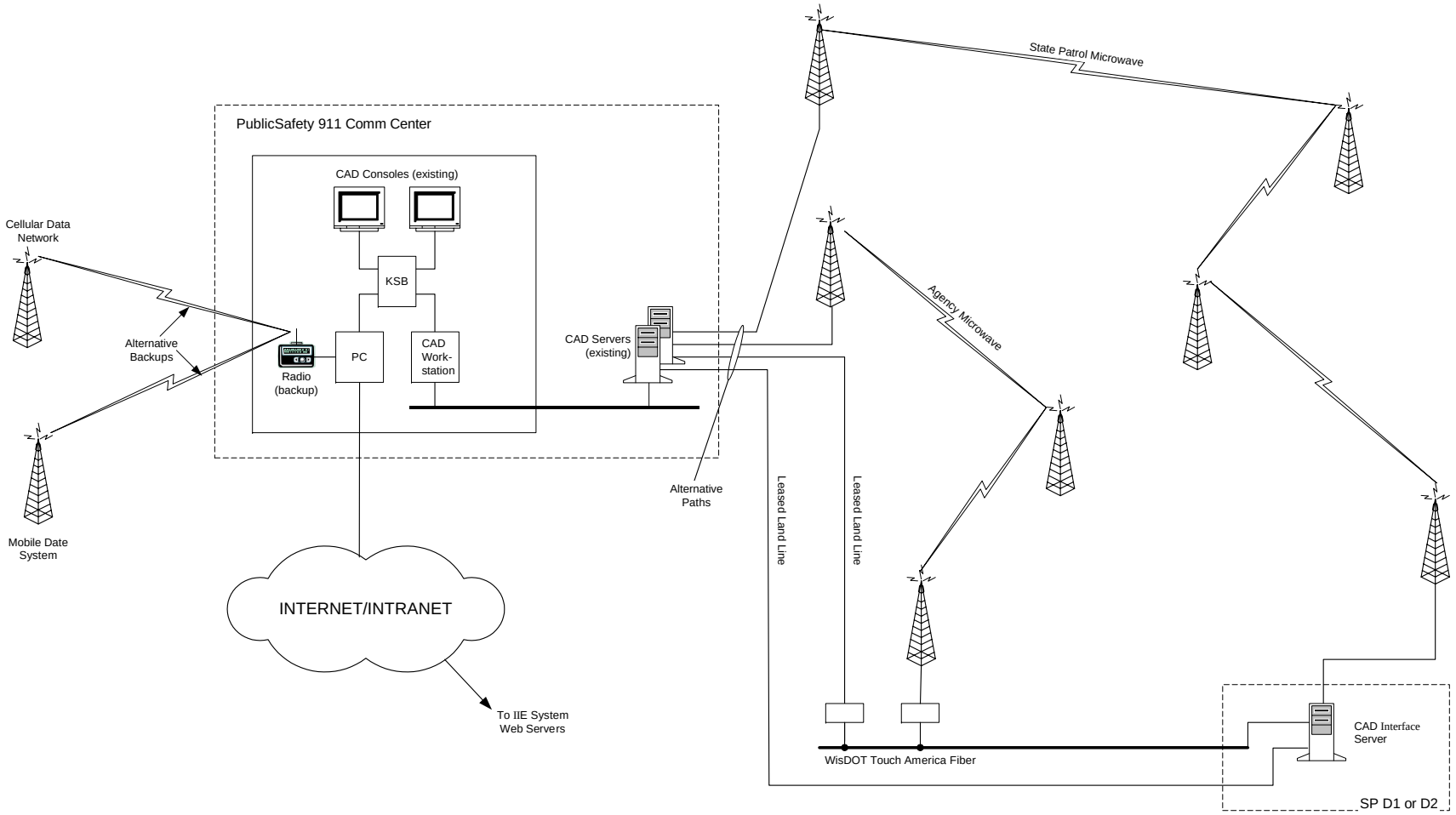

FIGURE 6.2-2
CAD SYSTEM INTERFACE

M:\WiSDOT\CAD SystemInterface.vsd
02/16/05

- If the number of highway incidents handled by a particular agency is low, it may be more cost effective to manually re-enter incident data into the IIE system on the rare occasions that such incidents occur.

Use of point-to-point communication circuit connections (as opposed to a shared medium, like the Internet) will likely be the connection method preferred by most agencies. A private point-to-point circuit will ensure that there is no public access to the CAD systems, or the criminal data and information on ongoing law enforcement activities that these systems contain. Since these connections are primarily used for the limited exchange of text data, typical voice-grade or DS0 digital circuits should suffice. Additional bandwidth would be required for the exchange of pictures and video.

Figure 6.2-2 illustrates several alternative communication circuit configurations for implementing the CAD system to IIE system link:

- Leased telephone line circuits from the CAD system location to the two CAD Interface Server locations.

- Leased telephone circuits from the CAD system location to the nearest access point on WisDOT's Touch America fiber, and then use of circuits on the fiber directly to the CAD Interface Server locations.

- Use of circuits on the agency's microwave system to the nearest access point on WisDOT's Touch America fiber, and then use of circuits on the fiber directly to the CAD Interface Server locations.

- Use of circuits on the State Patrol microwave system, either to a dropoff point on the WisDOT Touch America fiber, or all the way back to the CAD Interface Server locations at the State Patrol facilities.

The best communication circuit configuration for an agency's CAD system interface will have to be determined independently for each agency. This analysis will be based on the proximity of the agency to each communication resource and the availability of capacity on that resource to carry the additional data traffic. Where possible, diverse routes should be implemented between the CAD system and each of the redundant IIE system CAD Interface servers. This could involve using two different circuit configurations.

6.2.2.2 Public Safety Agency User Interface

If development of a link between a Public Safety CAD system and the IIE system is technically feasible and cost effective, the primary Dispatcher User Interface for incidents should continue to be the CAD displays. However, if a direct CAD-to-IIE interface is not implemented, or if the Public Safety Dispatcher needs to access other IIE system functions that are not supported by CAD (e.g., messaging, alerts, whiteboard, chat), the Dispatcher will need to have access to a monitor that has a

secure connection to the Public Internet or a state-wide WisDOT- or BadgerNet-based Intranet. Once such access is developed, all IIE system functions will be accessible to a user through a standard web browser.

The design for providing Internet or Intranet access to each user position will vary by agency. According to the WIJIS workgroup study for the Justice Information Sharing Initiative, 79% of the State's Sheriff departments and 89% of the State's Police agencies already have Internet access. Two-thirds of all law enforcement agencies have access to the State's fiber optic SONET network, BadgerNet. No data was provided on the distribution of this access to individual dispatch positions.

Most public safety agencies will want to maintain isolation of their CAD system from these shared external networks. So even if the CAD workstations are Internet capable, the agency will not want to tie the Internet or a state-wide Intranet into their CAD LAN. The simplest solution is to run a parallel LAN within the dispatch center and add a PC and monitor to each dispatch position. This parallel network may already exist in some dispatch offices to provide office type applications throughout the dispatch center (e.g., email, word processing, Internet). Typically, however, dispatch console space is at a premium and there is insufficient room to add another monitor to each dispatch position. An alternative design is illustrated in Figure 6.2-2, whereby the Internet/Intranet accessible PC shares the monitor/keyboard/mouse with the CAD system using a KVM switch. This design provides isolation for the CAD system as these peripherals are never "attached" to both the CAD system and Internet/Intranet PC at the same time.

At least a few dispatch positions in each Communication Center should have a backup path to the IIE system if the primary shared network path is down, or if commercial Internet service is disrupted. One solution would be to have a few portable mobile data computers (including radio) in the Communication Center that could be brought out when such failures occur. Figure 6.2-2 illustrates an alternative approach that interfaces a mobile data system radio directly to the Internet/Intranet PC. This radio could be connected to the agency's mobile data system, the State Patrol mobile data system, or a commercial cellular network.

All Public Safety agency interfaces to the public Internet, or even a less- accessible Intranet, and the IIE system must be secure. Typically agencies will implement appropriate firewalls in their Internet interfaces as normal good practice. However, in addition to firewall protection, communications between each user's PC and the IIE system should utilize a secure protocol, such as VPN (Virtual Private Network). VPN is a technology that establishes a secure "tunnel" to connect two points across a shared public network (i.e., Internet). Data sent across the shared network is encrypted and is "invisible" to other users on the shared network. VPN technology is widely available.

It is clearly evident from the discussion above, that several alternatives exist to providing Public Safety Communication Center or agency access to the IIE system. Each participating Center and Public Safety agency will need to be individually evaluated for determination of the best approach, or combination of approaches, to implement.

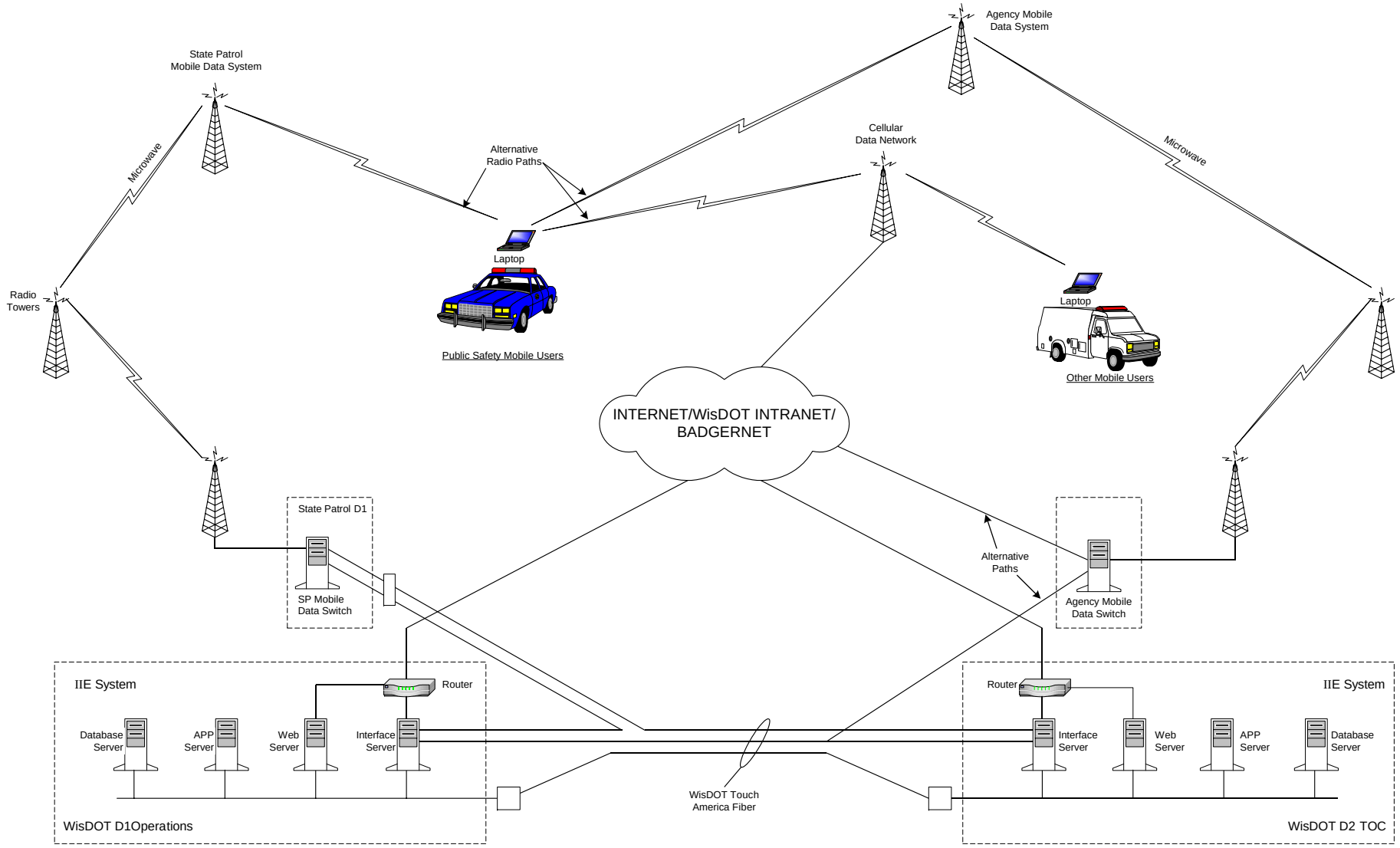

FIGURE 6.2-3
MOBILE DATA CONCEPTUAL CONFIGURATION

M:\WiSDOT\MobileDataConceptualConfig.vsd
02/16/05

6.2.3 Public Safety Mobile Data System

Figure 6.2-3 illustrates the conceptual design for the interface of mobile data users and systems to the IIE system. Similar to land-based users, the objective of the IIE system conceptual design is to minimize the need for any special or additional mobile data computer hardware or software to provide access to the IIE system functions. This approach will minimize the initial investment and support costs for each participating agency, thus reducing or eliminating barriers to participation. This approach is also vital for practical management of the potentially very large IIE system mobile user community. However, unlike land-based users, the bandwidth limitations of over-the-air data transmissions have, in many cases, lead to proprietary mobile data protocol and software solutions, posing challenges for meeting the minimum customization objective. Wherever possible, any customization needed to support a IIE system interface should occur in the agency's mobile data switch, rather than the mobile data computers.

6.2.3.1 Mobile Data Network Alternatives

For Public Safety mobile users, there are basically three different types of mobile data networks that can provide access to the IIE system functions:

- Public Cellular Data Networks (public 802.11 hot spots, metropolitan networks, and mesh networks would be included in this category)
- Private Agency-owned Mobile Data Radio Network
- State Patrol Mobile Data Network

The following sections describe these three alternatives. Each agency should be individually evaluated to determine the viable and best network, or combination of networks to use to provide mobile users with access to the IIE system.

6.2.3.1.1 Public Cellular Data Networks:

Mobile data systems that use public cellular data networks should be adaptable to interface to the IIE system. These cellular networks already provide Internet access. Even if these networks are being used in a proprietary manner, it should be possible to set up a separate software or hardware "port" to provide the Internet access. Similar to land-based computers, the mobile data computer should use VPN to encrypt data transmissions and establish a secure connection with the IIE system.

The latest cellular data networks support the high data rates that would be required for the map-based and high graphic content (e.g., pictures, video) applications on the IIE system. Until more wideband private radio technologies become prevalent, such as the emerging technology to combine channels in the 700 MHz band, cellular data networks will be an attractive solution for supplementing IIE system access for private mobile data systems as well.

6.2.3.1.2 Private Agency-owned Mobile Data Radio Network

The most common Public Safety mobile data system design employs a private mobile data radio network, owned and operated by a Public Safety Agency or by a group of agencies (such as a county system). These designs can be deployed in any of the land mobile radio frequency bands (e.g., VHF, UHF, 800 MHz). Typically these systems are limited to 19.2 Kbps data rates, or less. These data rates can support text-based Public Safety applications, such as motor vehicle checks, AVL, queries to State and National crime databases, Hazmat material information, and vehicle-to-vehicle text messaging. However, these data rates, particularly when shared by multiple vehicles, are not sufficient to transfer highly graphical data, such as maps, photographs, fingerprints, building plans, and of course video. New mobile data radio technologies, such as those being deployed in the 700 MHz band (see Section 5.1 above) will support much higher data rates, making the future exchange of graphical data possible.

Because of the bandwidth limitations of private mobile data radio systems, vendors have developed extremely efficient, and proprietary over-the-air protocols to maximize the number of users that can be supported by the system, and to minimize response times to officer queries. These systems are designed specifically to support the transfer of known data sets. The proprietary protocols require complimentary proprietary applications on the vehicle mobile data computer to correctly interpret and display the transferred data. This is in contrast to web-based data transmissions, where all the information necessary to interpret and display the transmitted data is packaged in the transmission. Driving these proprietary networks are proprietary message switches. The message switch functions to repackage data to/from the format sent over the air to the mobile data computers, from/to the format used to communicate with the target computer (e.g., crime database).

The advantage of these proprietary designs is the ability to squeeze more data across data radio channels than could be achieved by more "open" computer industry approaches and protocols. The down side of these designs is the total lack of interoperability among mobile data systems developed by different vendors.

The conceptual design for providing IIE system functions to private mobile data network users will depend on the technology employed in that particular agency's mobile data system. There basically are two different approaches:

a. Mobile Data Systems using Open Standards: Many of the newer mobile data system designs utilize IP-addressable digital radio equipment and have message switches that can support the translation of the over-the-air protocol to standard Internet protocols. These systems will support the use of a browser on the mobile data computer to view web-based applications on the Agency's Intranet or the public Internet. The transmission between the message switch and the mobile data computer is still proprietary, but this is totally transparent to both the field user and the application. These types of private radio network mobile data systems will be relatively easy to interface to the IIE system via Intranet or the Internet. The major accommodation necessary for these types of mobile

data systems will be to develop a parallel set of IIE system web-based displays that are designed specifically for the slower data rates of the private mobile data radio systems. These displays would be more text-based, and have minimal graphical data content compared to IIE system displays that would be used by fixed-site users. One set of displays would service all mobile data systems that fall in this category.

b. Proprietary Mobile Data Systems: Mobile data systems that use proprietary technologies throughout the message switch, over-the-air protocol, and mobile data computer present a more difficult challenge to interface to the IIE system. These systems cannot present a transparent connection between the Internet/Intranet and the mobile data computer. For such highly proprietary systems, significant customization will be required to deliver the IIE system functionality to the field. CAPWIN, a data interoperability project in the greater Washington DC area faced a similar dilemma. Their solution was to develop custom translation software for each mobile data system. This software, called the "CapWIN Connector" is resident in the message switch, and performs the function of translating CAPWIN data and displays into a form that can be transferred across the mobile data radio network and properly interpreted and displayed on the mobile data computer. Unique CapWIN Connector software had to be developed for each mobile data system. The CapWIN Connector was designed to provide a standard interface to the central CapWIN system. With this approach, there was no mobile data system-specific customization required for the central system. All mobile data systems "appeared" identical to the central system. A major upgrade/replacement of a mobile data system would be transparent to the central system.

   This message switch based translation software approach is recommended for interfacing proprietary mobile data systems to the IIE system. This approach, however, can be costly and carries the risk that is associated with any major software development. It will only be cost-effective for larger departments (or groups of agencies) using mobile data systems that have substantial remaining service life. For smaller departments, a dual-radio approach will likely be more cost effective. This approach uses the routing capabilities of most modern mobile data computers, along with a second data radio. All IIE system transactions would use this second radio network. This routing approach is described in Section 6.2.3.1.4 below.

Regardless of the degree of proprietary technology used by a particular mobile data system, its ability to interface to the IIE system will be strongly influenced by the availability of spare capacity to support the data transmission requirements of the IIE system functions. None of the mobile data systems in Wisconsin were designed with IIE system requirements in mind. Prudent planning may have provided spare capacity for unplanned future applications that could be utilized for IIE system transmissions. Many systems, however, may be operating at capacity. The IIE system mobile data transmission requirements are not significant, particularly if the more efficient text-based user interfaces are employed. Because of

IIE system's predominant use for incident response, its data transmission requirements can peak for short periods of time, but present a low average additional load to the system. An incident that attracts a large number of responders into one small geographical area could temporarily overload the mobile data system's resources in that area. A mobile data system with moderate spare capacity that is designed to handle such dynamics should be able to accommodate the addition of IIE system functions. Systems that are operating near capacity should consider the multiple-radio routing approach described in Section 6.2.3.1.4 below.

6.2.3.1.3 State Patrol Mobile Data Network

The existing State Patrol mobile data network is limited to 4800 bps over-the-air data rates. State Patrol is currently converting this system to a new IP-based mobile data system running at 19.2 Kbps. In the vehicle, the mobile data computer's Ethernet port will connect directly to an IPMobilenet data radio; a TCP/IP socket will be used to communicate via IP to the message switch. No middleware is required. The new State Patrol mobile data system is an example of a private "mobile data radio system using Open Standards" (Section 6.2.3.1.2.a). The system can support web-based applications and provides an ideal architecture for interfacing to a future IIE system, using the more efficient "text-based" web displays.

As indicated in Section 4.3.1 above, the State Patrol mobile data system is used by approximately 144 state, county local, tribal, and federal agencies throughout Wisconsin. There are approximately 1300 mobile data computers on the system and approximately 350 mobile data computers are typically logged in at any one time. Because of the large number of users, and the bandwidth limitations of the existing 4800 bps system, non-State Patrol users were limited to criminal and motor vehicle database query applications. While the move to 19.2 kbps will provide additional bandwidth, new law enforcement applications, including low-resolution photographs, are already planned and being deployed that will take up most of the new capacity. So while an interface to the IIE system is technically feasible, any widespread deployment of IIE system functions will be constrained by system bandwidth. This functionality may be initially provided to State Patrol officers and selected agencies in areas where there are high numbers of highway incidents, but it may be necessary to block access to IIE system applications by other agencies that share the mobile data system.

Long term, State Patrol is looking at higher bandwidth alternatives for mobile data, such as the 700 MHz spectrum, to meet the high data needs for future law enforcement applications, including fingerprint identification and video. Assuming the State Patrol will continue to provide mobile data service for other Law Enforcement agencies throughout the state, there is an excellent opportunity to provide widespread mobile data access to the IIE system applications if the planning and future evolution of the State Patrol mobile data system includes the data needs of these applications in its design.

6.2.3.1.4 Use of Multiple Mobile Data Networks

The best data network approach for a particular agency may be combination of the three mobile data network alternatives described above. As indicated in Section 5.1, most modern mobile data computers have the ability to simultaneously support, or at least switch among multiple radio system connections. Routing software on the mobile data computer enables the use of different radio systems for each mobile application. These routing features can be used to support several different combinations of mobile data computer communication configurations, as illustrated in the Table 6.2-2 below:

Table 6.2-2
Alternatives Data Network Configurations for
IIE System Mobile Data Access

Configuration Alternative	Cellular Data Network	Private Mobile Data Network	State Patrol Mobile Data Network
1	• Law Enforcement Apps • IIE System Apps		
2		• Law Enforcement Apps • IIE System Apps	
3			• Law Enforcement Apps • IIE System Apps
4	• IIE System Apps	• Law Enforcement Apps	
5	• IIE System Apps		• Law Enforcement Apps
6	• IIE System high-bandwidth Apps	• Law Enforcement Apps • Text-based IIE system apps	
7	• IIE System high-bandwidth Apps		• Law Enforcement Apps • Text-based IIE system apps
8	• IIE system Apps	• Law Enforcement Apps • **Backup** Text-based IIE system apps	
9	• IIE system Apps		• Law Enforcement Apps • **Backup** Text-based IIE system apps
10		• Law Enforcement Apps • IIE System Apps	• **Backup** Law Enforcement Apps • **Backup** Text-based IIE system apps

Alternatives 1, 2, and 3 show the addition of the IIE system applications to whatever mobile data communications network is currently being used by the agency. This approach is most suitable for modern and new mobile data systems that have excess spare capacity or have planned in advance to make provisions for IIE system applications.

Alternatives 4 and 5 retain the Law Enforcement applications on the existing mobile data network, and utilize the cellular data network for the new IIE system applications. This may be the easiest and most cost/effective approach to adding IIE system capabilities to older mobile data systems, mobile data systems that are not readily adaptable to IIE system protocols, or mobile data systems that have limited or no spare capacity to implement new functions. This approach can be rapidly deployed for pilot

testing prior to investing in mobile data system modifications or radio network upgrades. It can also be used as a temporary holdover solution until an existing private mobile data system is slated for replacement.

Alternatives 6 and 7 illustrate the use of cellular data networks for the high bandwidth IIE system applications, while keeping Law Enforcement and mission critical IIE system applications (text-based) on a private mobile data network. This approach uses each type of mobile data network for its particular strengths: mission critical applications use the highly secure and reliable private network; the less critical, graphically-oriented applications use the higher bandwidth, but less reliable public network.

Alternatives 8, 9, and 10 illustrate the use of the mobile data computer routing capability to provide backup paths for applications if the primary mobile data network fails. The higher bandwidth IIE system applications do not failover in these alternatives, so as not to impact normal communications on the backup network with excessive data transfers.

6.2.3.2 Mobile Data System Message Switch Interface

The design for the interface between an agency's mobile data message switch and the IIE system must consider many of the same issues that impact the design of an Agency's CAD system to the IIE system. Mobile data systems carry criminal and homeland security data that must be protected from outside access. Mobile data systems, because they transfer this data over the public airwaves, must address these security concerns on a daily basis. For example, FBI standards for encryption must be followed for any mobile data system that provides access to National crime databases.

Because of the issues that a mobile data switch interface to the IIE system shares with the CAD interface, use of point-to-point communication circuit connections (as opposed to a shared medium, like the Internet) will also be the most likely connection method preferred by most agencies. A private point-to-point circuit will ensure that there is no public access to the mobile data switch. Unlike the CAD system interface, however, a high bandwidth connection will be needed between the mobile data switch and the IIE system to support the web-based user interface. A fractional-to-full T1 circuit is recommended. Since the conceptual user interface design employs web-based technologies, the protocol for the message switch to IIE system interface should be TCP/IP over Ethernet. Data encryption should be retained over the connecting circuit. If a shared medium is used, a VPN, or similarly secure connection should be established between the message switch and the IIE system interface server.

As indicated in Section 6.2.2.1, there are several alternative communication circuit configurations for implementing a point-to-point interface for the mobile data switch to IIE system link. Unlike the CAD system link, which can utilize a lower speed circuit, the higher data rates needed for the mobile data switch may eliminate some of the microwave path alternatives due to the more limited bandwidth of these alternatives. Alternative circuit configurations include:

- Leased circuits from the message switch location to the two Interface Server locations.

- Leased circuits from the message switch location to the nearest access point on WisDOT's Touch America fiber, and then use of circuits on the fiber directly to the Interface Server locations.

- Use of circuits on the agency's microwave system to the nearest access point on WisDOT's Touch America fiber, and then use of circuits on the fiber directly to the Interface Server locations.

- Use of circuits on the State Patrol microwave system to a dropoff point on the WisDOT Touch America fiber.

The best communication circuit configuration for an agency's message switch interface will have to be determined independently for each agency. Similar to the CAD system interface, this analysis should be based on the proximity of the agency to each communication resource and the availability of capacity on that resource to carry the additional data traffic. Where possible, diverse routes should be implemented to each of the redundant IIE system Interface Servers. This could involve using two different circuit configurations.

6.2.4 Non Public Safety User Interface

Transportation and other non-Public Safety users must be able to access IIE system functions from any location, including their desks, vehicle, home, Transportation Operation Centers, mobile incident command vehicles, and Emergency Operation Centers. While dedicated point-to-point circuits could be employed, this approach constrains mobility, would be extremely expensive (particularly for high data rate circuits), and would be difficult to manage (e.g., addition of new users, deletion of old users, users moving locations). The recommended approach for the conceptual design is to utilize the Public Internet (wide-band, where available), or where accessible, WisDOT- or BadgerNET-based Intranets for these user groups. Mobile users that do not have access to a private mobile data system should use cellular data networks. Cellular data networks should also be considered as a backup Internet path for fixed-site users. VPN, or similar technology, should be used to establish a secure, encrypted connection across the shared network between the user's device and the IIE system.

6.2.5 Traffic Management System Interfaces

It is anticipated that WisDOT's Traffic Management Systems will undergo considerable evolution prior to implementation of the IIE system as a result of the future studies recommended by the WisDOT State Traffic Operations Plan (TOPS). This plan identified several studies to occur over a three-to-four year period to develop state-wide standards for highway operations and related ITS systems. The IIE system requirements will be an important input to these planning processes; the output of these processes will impact the IIE system design, including the number and types of interfaces that will be required for the IIE system.

The IIE system design, at the conceptual level, will interface to WisDOT's traffic management systems, as necessary, to make available highway operations data to the IIE system users. This data will include road weather, traffic conditions, variable message sign settings, planned and realtime events, incidents, and traffic video. It is anticipated that, in comparison to the Public Safety CAD and mobile data system interfaces, the number of traffic management system interfaces will be small, and can be can be cost/effectively customized as necessary. These interfaces should utilize National and State ITS Architecture protocol standards, as determined by the TOPS planning initiatives.

It is anticipated that the evolution of the state's traffic management systems will be in a direction to provide greater access to its information via web displays. The IIE system, as well, will utilize web displays and services as its primary means of disseminating information to IIE system users. Wherever possible, the IIE system should directly utilize links to the traffic management web sites, rather than attempt to duplicate these functions.

The conceptual design assumes key traffic management systems will continue to be located at the WisDOT District 2 Traffic Operations Center, and the District 1 office (or WisDOT Hill Farms facility) in Madison. The conceptual design recommends that key centralized components and servers of the IIE system be located at these facilities to provide an opportunity for localized interfaces, and because of the availability of local support staff. The outcome of the TOPS-initiated studies may recommend alternative configurations and/or locations for future traffic management systems in the state. The IIE system conceptual design recommendations will need to be re-evaluated based on these TOPS-initiated study recommendations.

To date, WisDOT has addressed the desire of specific Law Enforcement agencies to have access and control of highway video cameras by implementing agency-specific point-to-point designs using existing fiber infrastructure, occasionally supplemented with short runs of newly-installed fiber facilities. These designs provide agency access to the video feeds by providing direct access to WisDOT's video switching hardware. While this approach can continue to provide high-quality video feeds to some Law Enforcement agencies in the state, particularly agencies that have facilities close to WisDOT's fiber infrastructure, it cannot serve as a general model to provide video to all potential IIE system users across the state. The only practical means to meet the state-wide access need is to provide this capability via the Internet. The continued expansion in availability of wide-band access to the Internet, and continued improvements in video compression and streaming video on the Internet, should make this design for providing state-wide access to high quality video a viable design in the not-to-distant future.

Although the TOPS planning efforts may have some impact the conceptual design presented in this report, it will likely have far greater impact on the subsequent detailed design phases of the IIE system. The following TOPS planning efforts and studies could impact the detailed IIE system design:

- Data Management Plan: This plan will include a WisDOT data dictionary and related data storage, reporting, and archiving requirements. The standards, plans, and data dictionary outputs of this plan will need to be incorporated into the IIE system design.

- Infrastructure strategic Plan: The IIE system design will need to be compatible with the recommendations of the plan for infrastructure standards and expansion. Depending on the plan, deployment of the system may have to wait for development of the needed infrastructure, or the project itself may need to incorporate portions of the infrastructure expansion in its design.

- Traffic Operations Maintenance Management Plan: The final recommendations on this plan may impact the IIE system design. For example, it may be desirable to have the system hosted and maintained by an application service provider.

- Special Events Management Plan: The recommendations of this plan may impact design of the Traffic data interface.

- Traffic Operations Data Needs: This study will define traffic operations' data collection, reporting, and analysis standards. Additional information requirements may come out of this study that need to be incorporated into the IIE system design.

- Information Improvement Program: Traveler information improvements addressed by this plan include coordination and dissemination of traveler information. The recommendations of this plan will impact the way that the requirements for dissemination of Traffic information are handled in the IIE system design.

- Enhanced Web Access to Highway Operations Information: The web standards and information dissemination recommendations developed by this study will impact the IIE system design. Much of the information needed by the Public Safety community could be provided directly by other projects recommended by this study.

- Incident Management: This study may impact IIE system requirements. Since a major role of IIE system is to provide data interoperability in support of the realtime response to highway incidents, the IIE system requirements will also be a major input into the Incident Management Study. Unlike Public Safety CAD systems, where highway incident management is only one of many functions, the role any future WisDOT incident management system would have nearly total overlap with the incident management functions that the IIE system would provide. The IIE system design should be modified as necessary to directly meet WisDOT's needs for realtime incident management information and communications. It should not be necessary to have a separate Traffic Management incident management system, to which the IIE system has an interface.

- Development of Traffic Operations' Infrastructure: This study may recommend alternative standards in order to achieve compatibility objectives. These and other developed standards will need to be incorporated into the IIE system detailed design.

- Transportation security and Emergency Preparedness: The study recommendations may pose additional security requirements on the detailed IIE system design.

6.2.6 Conceptual Design Redundancy and Backup Considerations

As described above in the conceptual hardware design descriptions, and shown in the conceptual IIE system configuration diagrams, the IIE system servers and backbone infrastructure are designed with full redundancy of all servers and communication interfaces. To meet disaster recovery requirements, redundant elements should be located in different facilities. Any complement of servers should be able to provide full IIE system functionality. It should not be necessary to failover all servers from one site to the backup site upon the failure of a single server; only that individual server should failover to its backup at the alternate site. Complete failover to the backup site should only occur upon a disaster at one of the sites (e.g., fire, flood, terrorist bombing, major extended power outage).

The conceptual configuration diagrams also show alterative communication paths for interfacing IIE System users and Public Safety CAD systems to the IIE System server farms. The level of redundancy and diversity of communication paths that are ultimately implemented for each agency will depend on each agency's individual objectives and available resources (e.g., funding, access to communication facilities).

6.2.7 Summary of Public Safety Interface Issues

Because of variations in CAD and mobile data system implementations among Public Safety agencies, the conceptual design described in the sections above identifies several different alternatives for implementing these interfaces and identifies the system, infrastructure, and facility criteria that will determine the best solution. It will be necessary to individually evaluate each Public Safety agency to determine the best approach. The issues to be evaluated and the impact of those issues are summarized in Table 6.2-3.

Table 6.2-3
Public Safety Agency-Specific
Conceptual Design Issues

Agency Issue	Impacts
Ability of agency's CAD system to support a IEEE 1512 interface	Whether to implement a IEEE 1512 interface on the existing CAD system or wait until the system is replaced as part of its normal life cycle.
Statistics on the number of highway incidents handled per year	Whether there are sufficient number of incidents/year that the time savings from eliminating double entry of incident data into the CAD and IIE systems can justify the cost of implementing a IEEE 1512 interface for the CAD system.
Spare channel capacity in agency's microwave system and proximity of that system to WisDOT State Patrol microwave or fiber facilities.	Routing of CAD and mobile data switch interfaces to the IIE system.

Agency Issue	Impacts
Proximity of agency's dispatch location to WisDOT State Patrol microwave or fiber facilities	Routing of CAD and mobile data switch interfaces to the IIE system.
Availability of Internet/Intranet at Dispatch consoles	Best way to deliver IIE system user interface to the dispatcher.
Use of Cellular Data Network or Private Data Network for the agency's mobile data system.	Provision of backup user interface access to the IIE system if the primary Internet/Intranet access is out of service.
Proprietary features of the agency's mobile data system, including the ability of agency's mobile data system to provide transparent end-to-end IP connectivity.	• The complexity and hence cost of developing translation software for the mobile data message switch. • Evaluation of interface alternatives, including installing a cellular radio network modem in each vehicle and using the routing capabilities of the mobile data computer to route IIE system functions over the cellular data network.
Age of mobile data system, data rates, spare capacity, and number of mobile data computers.	Evaluation of interface alternatives, including installing a cellular radio network modem in each vehicle and using the routing capabilities of the mobile data computer to route all, or just high bandwidth IIE system functions over the cellular data network.
Proximity of dispatch office to WisDOT fiber	Whether a direct interface to WisDOT CCTV video switch is feasible to provide high quality traffic video.

6.3 Software Architecture

The IIE system software architecture design should not be overly restrictive. Ultimately, when the IIE system is put out for bid, the technical specification should focus on required functions, standards, and performance. Prospective bidders should be encouraged to propose designs that provide the specified functions and meet the required standards and performance while taking maximum advantage of the bidder's standard software designs and off-the-shelf software products. This approach will minimize project cost and risk, and result in a system that can be more easily supported and upgraded over its service lifetime. The software architecture, however, will need to have the following characteristics to meet not just functions, but the overall objectives for the IIE system:

a. Client/Server Architecture: Since the potential IIE system users could number in the thousands, any attempt to distribute application software among the users would be impractical to manage. Application software should be resident and execute in centralized servers. No IIE system-specific software should be necessary on the users' (clients) computers, as further discussed in (b) below.

b. Web-based User Interface and Services: The IIE system user interface should be fully accessible through the use of a standard Internet browser (e.g., Netscape, Microsoft Internet Explorer).

c. Scalable: The IIE system should be scalable to support an expanding base of participating agencies and users and to support a gradual rollout of the IIE system on a regional or corridor basis.

d. Configurable: The software cannot be designed with a "one size fits all" strategy. The IIE system functionality should be highly configurable on an agency and regional basis to best reflect the differences in organizational characteristics and processes that exist across the state.

e. GIS Orientation: The IIE system database and functions should have a strong GIS orientation. Wherever practical, responders, resources, events, and incidents should be tied to geographical coordinates and displayed on a map display.

f. Security: Many sections of this report have identified security requirements for the IIE system. The IIE system software must be designed from the ground-up with these security requirements in mind. For example, the IIE system database itself should be encrypted, so even if access security measures are compromised, a cyber attacker cannot get access to system data, or on a more routine level, a vendor's programmer could be able to perform software maintenance on the system without being able to read any of the system data.

g. Database Architecture: Data structures should conform to the National, State, and Regional ITS Architecture standards.

h. Standard Public Safety Mobile Data System Interface: In order to provide a standard TCP/IP interface to Public Safety mobile data systems, any customization required should be implemented in the mobile data system message switch. Using this approach, all mobile data system interfaces will be identical and should appear simply as additional Internet/Intranet users to the IIE system. Public Safety mobile data systems can be replaced or upgraded transparently to the IIE system.

6.4 Conceptual Design Summary

The conceptual design achieves data interoperability among Public Safety agencies and agencies involved with highway operations through the use of an information exchange hub, named the IIE system. The IIE system will consist of multiple servers to host the IIE application software and databases, provide interfaces to other systems, and service the web-based user interface for all system users. Servers should be redundant for high availability with the redundant servers located in geographically separated facilities to ensure survivability of the system if a man-made or natural disaster destroys or significantly impacts one of the locations. With the exception of servers that will interface to Public Safety CAD systems, preliminary recommendations for server locations are the WisDOT District 2 TOC and the WisDOT District 1 office or Hill Farms facility in Madison. CAD Interface Servers should

be located at law enforcement facilities, such as State Patrol District offices, where they will be under law enforcement control. The WisDOT fiber communications infrastructure should be used to provide high-speed communications among the servers.

Interfaces between Public Safety CAD systems and the IIE system should use point-to-point communication circuits and the IEEE 1512 protocol, designed specifically for this purpose. Interfaces between Public Safety mobile data systems and the IIE system can used point-to-point or shared communication circuits and Internet protocols (TCP/IP). Any translation software necessary to convert the Internet protocols to the proprietary over-the-air protocols used by the mobile data system should be resident in the mobile data message switch. This will provide a standardized interface at the IIE system that is independent of the proprietary mobile data systems that are used throughout the state.

Interfaces to WisDOT traffic management systems will be strongly impacted by the studies recommended by the Traffic Operations Plan. This plan identified several studies to occur over a three-to-four year period to develop statewide standards for highway operations and related ITS systems. The IIE system must interface to the systems that arise from these studies. With the objective of statewide standards for any such systems, the number of unique interfaces should be minimized (unlike the situation with the state's CAD and mobile data systems). The current practice of providing direct access to WisDOT's CCTV video switch hardware to provide high quality access to traffic video can continue for Public Safety agencies that have close proximity to WisDOT and other state fiber infrastructure, but cannot meet the needs for broader access to this video by IIE system users throughout the state. The conceptual design recommends that a more generalized Internet-based solution be implemented, taking advantage of constantly improving video compression and streaming technologies to provide high-quality video to any user with wide-band access to the Internet.

The IIE system software architecture should not be overly restrictive to allow for the maximum use of off-the-shelf software to minimize cost and risk. The software should be based on a client/server architecture and a web-based user interface. The software should be scalable, secure, and highly configurable. Data should have a strong GIS component, and be structured to meet National, State, and Regional ITS Architecture requirements, as well as any WisDOT data dictionary developed in the data studies arising from the TOPS plan.