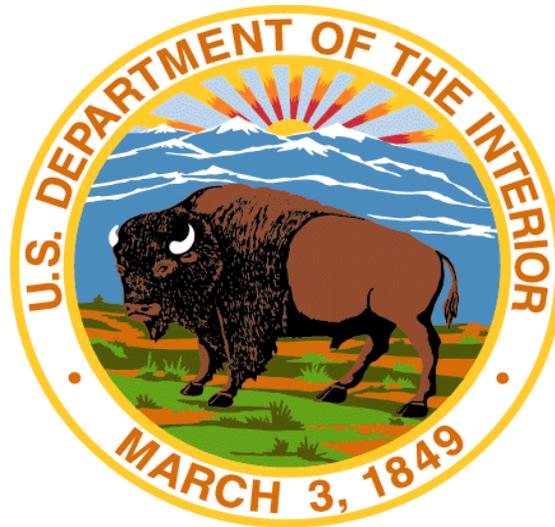


# **Department of Interior Enterprise Architecture (IEA)**



## **DOI Interior Enterprise Architecture Law Enforcement Modernization Blueprint**

### **Law Enforcement Line of Business**

Final – Version 1.1

November 2004

## Table of Contents

<b>1. BLUEPRINT INTRODUCTION .....</b>	<b>2</b>
<b>2. EXECUTIVE OVERVIEW .....</b>	<b>3</b>
<b>3. BUSINESS CONTEXT .....</b>	<b>5</b>
3.1    WHAT GOALS AND OBJECTIVES DOES THE DOI LAW ENFORCEMENT LOB SUPPORT? .....	5
3.2    WHAT FUNCTIONS DOES THE LAW ENFORCEMENT LOB PERFORM? .....	7
3.3    WHAT IT SERVICES ARE REQUIRED BY LAW ENFORCEMENT? .....	10
<b>4. FINDINGS AND RECOMMENDATIONS .....</b>	<b>15</b>
4.1    PROGRAM FINDINGS & RECOMMENDATIONS .....	15
4.2    SYSTEM FINDINGS & RECOMMENDATIONS .....	17
4.3    BUSINESS FINDINGS & RECOMMENDATIONS.....	21
4.4    DATA FINDINGS & RECOMMENDATIONS.....	24
4.4.1 <i>NPS Specific IMARS Interface Requirements</i> .....	27
4.4.2 <i>FWS / NWRS Specific IMARS Interface Requirements</i> .....	31
4.4.3 <i>BIA Specific IMARS Interface Requirements</i> .....	32
4.4.4 <i>BOR Specific IMARS Interface Requirements</i> .....	34
4.4.5 <i>BLM Specific IMARS Interface Requirements</i> .....	35
4.5    TECHNOLOGY FINDINGS & RECOMMENDATIONS .....	37
<b>5. TRANSITION PLAN .....</b>	<b>41</b>
5.1    TACTICAL RECOMMENDATIONS:.....	41
5.2    STRATEGIC RECOMMENDATIONS .....	43
<b>6. REFERENCES.....</b>	<b>45</b>
<b>APPENDIX A - SUPPORTING ANALYTICAL REPORTS DERIVED FROM THE DOI ENTERPRISE ARCHITECTURE REPOSITORY (DEAR).....</b>	<b>47</b>
<b>APPENDIX B - SUPPORTING ANALYTICAL REPORTS DERIVED FROM INTERVIEWS WITH LAW ENFORCEMENT LOB SYSTEM OWNERS, DEVELOPERS, AND USERS.....</b>	<b>48</b>
B-1. LEMIS 2000 APPLICATION .....	48
B-2. LE-IMAGS APPLICATION .....	52
B-3. LAWNET APPLICATION.....	52
<b>APPENDIX D – GLOSSARY OF TERMS .....</b>	<b>59</b>

## Table of Figures

<b>FIGURE 3-1. LAW ENFORCEMENT LINE OF BUSINESS PRM DIAGRAM.....</b>	<b>5</b>
<b>FIGURE 3-2. LAW ENFORCEMENT LINE OF BUSINESS BRM DIAGRAM .....</b>	<b>10</b>
<b>FIGURE 4-2. LAW ENFORCEMENT DATA SUBJECT AREAS.....</b>	<b>25</b>
<b>FIGURE 4-3. IMARS CONCEPTUAL SYSTEM INTERFACE DIAGRAM .....</b>	<b>26</b>
<b>FIGURE 4-4. IMARS NPS DETAILED SYSTEM INTERFACE DIAGRAM .....</b>	<b>28</b>
<b>FIGURE 4-5. IMARS FWS / NWRS DETAILED SYSTEM INTERFACE DIAGRAM .....</b>	<b>31</b>
<b>FIGURE 4-6. IMARS BIA DETAILED SYSTEM INTERFACE DIAGRAM.....</b>	<b>33</b>
<b>FIGURE 4-7. IMARS BOR DETAILED SYSTEM INTERFACE DIAGRAM .....</b>	<b>34</b>
<b>FIGURE 4-8. IMARS BLM DETAILED SYSTEM INTERFACE DIAGRAM.....</b>	<b>36</b>
<b>FIGURE 4-9. LAW ENFORCEMENT “AS IS” CONCEPTUAL SYSTEM ARCHITECTURE .....</b>	<b>38</b>
<b>FIGURE 4-10. DIAGRAM SHOWING RELATIONSHIP OF PATTERNS TO SOLUTION DEVELOPMENT PROCESS .....</b>	<b>40</b>
<b>FIGURE 5-1. LAW ENFORCEMENT “INTERIM” CONCEPTUAL SYSTEM ARCHITECTURE .....</b>	<b>42</b>
<b>FIGURE 5-2. LAW ENFORCEMENT NEAR-TERM “TO-BE” CONCEPTUAL SYSTEM ARCHITECTURE... </b>	<b>43</b>
<b>FIGURE 5-3. LAW ENFORCEMENT LONG-TERM “TO-BE” CONCEPTUAL SYSTEM ARCHITECTURE... </b>	<b>44</b>

## Table of Tables

<b>TABLE 3-1. RECREATION LOB END OUTCOMES MAPPED TO INTERMEDIATE OUTCOMES .....</b>	<b>6</b>
<b>TABLE 3-2. DESCRIPTION OF LAW ENFORCEMENT FUNCTIONS BY DOI BUREAU .....</b>	<b>7</b>
<b>TABLE 3-3. LAW ENFORCEMENT LOB SERVICE COMPONENTS.....</b>	<b>10</b>
<b>TABLE 3-4. SERVICE COMPONENTS MAPPED TO LAW ENFORCEMENT APPLICATIONS.....</b>	<b>13</b>
<b>TABLE 4-1. SERVICE COMPONENTS MAPPED TO LAW ENFORCEMENT APPLICATIONS.....</b>	<b>15</b>
<b>TABLE 4-2. COMPARISON OF IMARS AND BUREAU LE SYSTEM FUNCTIONALITY .....</b>	<b>16</b>
<b>TABLE 4-3. COMPARISON OF DOI LAW ENFORCEMENT SYSTEMS .....</b>	<b>17</b>
<b>TABLE 4-4. LAW ENFORCEMENT SYSTEM DESCRIPTIONS .....</b>	<b>18</b>
<b>TABLE 4-5. SERVICE COMPONENTS MAPPED TO LAW ENFORCEMENT APPLICATIONS .....</b>	<b>21</b>
<b>TABLE 4-6. LEVEL OF AUTOMATION OF LAW ENFORCEMENT FUNCTIONS BY DOI BUREAU .....</b>	<b>22</b>
<b>TABLE 4-7. CURRENT LEVEL OF AUTOMATION AND MISSION CRITICALITY OF LAW ENFORCEMENT FUNCTIONS .....</b>	<b>23</b>
<b>TABLE 4-8. IMARS CENTRAL SERVER SYSTEM INTERFACES .....</b>	<b>27</b>
<b>TABLE 4-9. IMARS NPS SYSTEM INTERFACES .....</b>	<b>29</b>
<b>TABLE 4-8 IMARS FWS / NWRS SYSTEM INTERFACES .....</b>	<b>32</b>
<b>TABLE 4-9 IMARS BIA SYSTEM INTERFACES.....</b>	<b>34</b>
<b>TABLE 4-10 IMARS BOR SYSTEM INTERFACES .....</b>	<b>35</b>
<b>TABLE 4-11 IMARS BLM SYSTEM INTERFACES.....</b>	<b>36</b>

# 1. Blueprint Introduction

The Law Enforcement Line of Business (LOB) Modernization Blueprint document identifies a series of existing architectural issues and opportunities for business improvement by evaluating strategic objectives, business functionality, technology, data, and systems that are used within the current business's operational architecture. The issues are generated by using a structured architecture methodology called a Target Application Architecture (TAA) methodology. This methodology collects the current architectural artifacts, validates them with the subject matter experts (SME) and then proceeds to evaluate and score the artifacts in the context of the LOB and enterprise requirements using the approved DOI evaluation criteria. The results of this scoring are analyzed to generate a list of potential improvements, that if rectified, present value to the LOB. The improvement opportunities are characterized as either tactical (addressable in a 1-2 year time frame) or strategic (addressable in 2-5 year time frame). Each finding is accompanied by recommendations on how to implement the solution. All the opportunities are rolled into an integrated transition plan to guide the evolution of the LOB's improvement strategies. The Blueprint will act as a series of planned steps that will transition the architecture toward its future target state. The Blueprint should be used by Business Owners, Portfolio Managers, Investment Managers, and System Owners as the means to ensure coordinated migration to the target state.

The Blueprint is comprised of five primary sections:

- Executive Overview - The Executive overview provides for a quick reference to the series of opportunities for improvement and a general context for maturity of the LOB.
- Business Context - The Business context provides for a brief description of the business functions and services that are provided and the strategic objectives that it is attempting to satisfy.
- Findings and Recommendations - The bulk of the report is the Findings and Recommendations (F&R) section that describes what the existing architecture issues are from a variety of perspectives. The F&R describes in the context of systems, technologies, data, business functionality, or strategic planning elements where improvements can occur due to redundancies, voids, or general industry trends. All the findings or opportunities are associated to specific recommendations on how to proceed.
- Transition Plan - The Transition Plan section describes the findings in the form of the integrated steps required to take the recommendations and begin to prioritize, develop business cases or investment proposals, initiate projects, or develop policy.
- Appendix A - Supporting Analytical reports derived from the DOI Enterprise Architecture Repository (DEAR) describing the analytical relationships between the system artifacts
- Appendix B – Supporting Analytical reports derived from interviews with Law Enforcement LOB system owners, developers, and users.
- Appendix C – Glossary of Terms

## 2. Executive Overview

The analysis of the Recreation LOB has yielded a series of findings and opportunities that have been arranged into the following classifications:

- *Program*: refers to general issue concerning, funding, planning, workforce, objectives, or communication and outreach
- *System*: refers to findings concerning the relative maturity of the deployed IT systems and how well they support the LOB mission
- *Business*: refers to the findings concerning functional activities or process findings that would facilitate improvements to the LOB
- *Data*: refers to the findings identifying opportunities for data sharing or data exploitation to improve business intelligence or efficiency
- *Technology*: refers to the findings where the LOB is dealing with non-standardized or obsolete technologies or architectures

Each finding is used to develop an integrated activity plan that will be used by the business owners to develop a prioritized strategy to drive the business improvement process. These activities may take the form of formal business case submission, business process re-engineering, systems integration, partnerships or policy development as well as other methods. The primary value of the integrated plan is to provide a management tool to ensure a coordinated vision and strategy for future investments and internal collaboration. The complete list of findings can be found in the summary tables. For a complete discussion of the opportunities, refer to the Findings and Recommendations Section.

### Program Findings

1. Current Law Enforcement Systems provide similar functions and services and are isolated along organizational boundaries. These redundancies and inefficiencies are being addressed by the planned Departmental IMARS procurement planned for early Fiscal Year 2005.
2. LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report; however LAWNET does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, report crime statistics to the DOJ/FBI through the Department.

### System Findings

1. Current Law Enforcement Systems support similar primary business functions.
2. Current Law Enforcement Systems provide / require similar information technology services.
3. Current Law Enforcement Systems are not integrated and have deployed non-shared, Bureau-system-specific infrastructure investments.

### Business Findings

1. Activities performed by Bureaus supporting the law enforcement LOB vary across the DOI, but there are core function activities that are suitable for cross departmental automation.
2. The planned IMARS procurement will provide a level of automation for core business functions across all Bureaus supporting the law enforcement LOB.

### Data Findings

1. There is clearly a need for a DOI-wide law enforcement data model. Physical data models of existing systems and a conceptual data model of the planned IMARS system will be necessary to

effectively plan any data migration and/or system integration. The FWS LE-IMAGS and the BLM LAWNET systems have an existing data model.

2. The planned IMARS system has extensive requirements for interfacing with existing DOI, Bureau, and external systems that span law enforcement, facilities management, asset management, and accounting. These interface requirements highlight the need for a published IMARS data model and DOI-wide standards for information exchanges between these systems.

### **Technology Findings**

1. Current Law Enforcement Systems are not integrated and have deployed non-shared, Bureau-specific infrastructure investments.
2. Only two systems, LEMIS and LE-IMAGS<sup>1</sup> (known internally as the LEMIS NWRS module or IMARS/FWS/RLE), use Active-Directory user authentication. All other law enforcement systems have individual means of tracking user authentication.
3. BLM's LAWNET and NPS's CIRS systems are based on end-of-life DOS technology.
4. NPS's CRIMES is based on MS Access database technology that has reached the 1GB database size limit of MS Access for certain larger National Parks.
5. The LEMIS and LE IMAGS systems are J2EE-compliant systems. In all instances where LEMIS and LE IMAGS modules have common business functions, only one instance of code is used and only one database component is used.
6. There are differences between IMARS Functional Requirements and Bureau-specific TRM implementations.
7. IMARS will address the system-specific infrastructures of the current environment by featuring reusable technical components in a standards-based solution architecture using patterns.

---

<sup>1</sup> LE IMAGS and LEMIS are system names taken from current published investment proposal (i.e. exhibit 300) documentation. It is understood that internally within the FWS, LE-IMAGS is called IMARS/FWS/RLE and that LEMIS is called IMARS/FWS/OLE. Changing the names of these systems to internally recognized acronyms may confuse the OMB, thus the original names were retained

### 3. Business Context

#### 3.1 What goals and objectives does the DOI Law Enforcement LOB support?

The Department of the Interior’s (DOI) Integrated Performance Reference Model (PRM) is an extension of the OMB’s FEAPMO PRM. The PRM is a standardized measurement framework to characterize performance in a common manner. The DOI Integrated PRM contains elements of the DOI’s Strategic Plan and DOI ABC Work Activities, which reflect the indirect and direct influences associated with the broad Recreation stakeholder community.

The DOI Integrated PRM links DOI ABC Work Activities to the DOI Strategic Plan goals and objectives that a given work activity supports. The Performance Reference Model diagram, Figure 3-1, graphically shows the End-Outcome and Intermediate-Outcome goals associated with the Law Enforcement LOB.

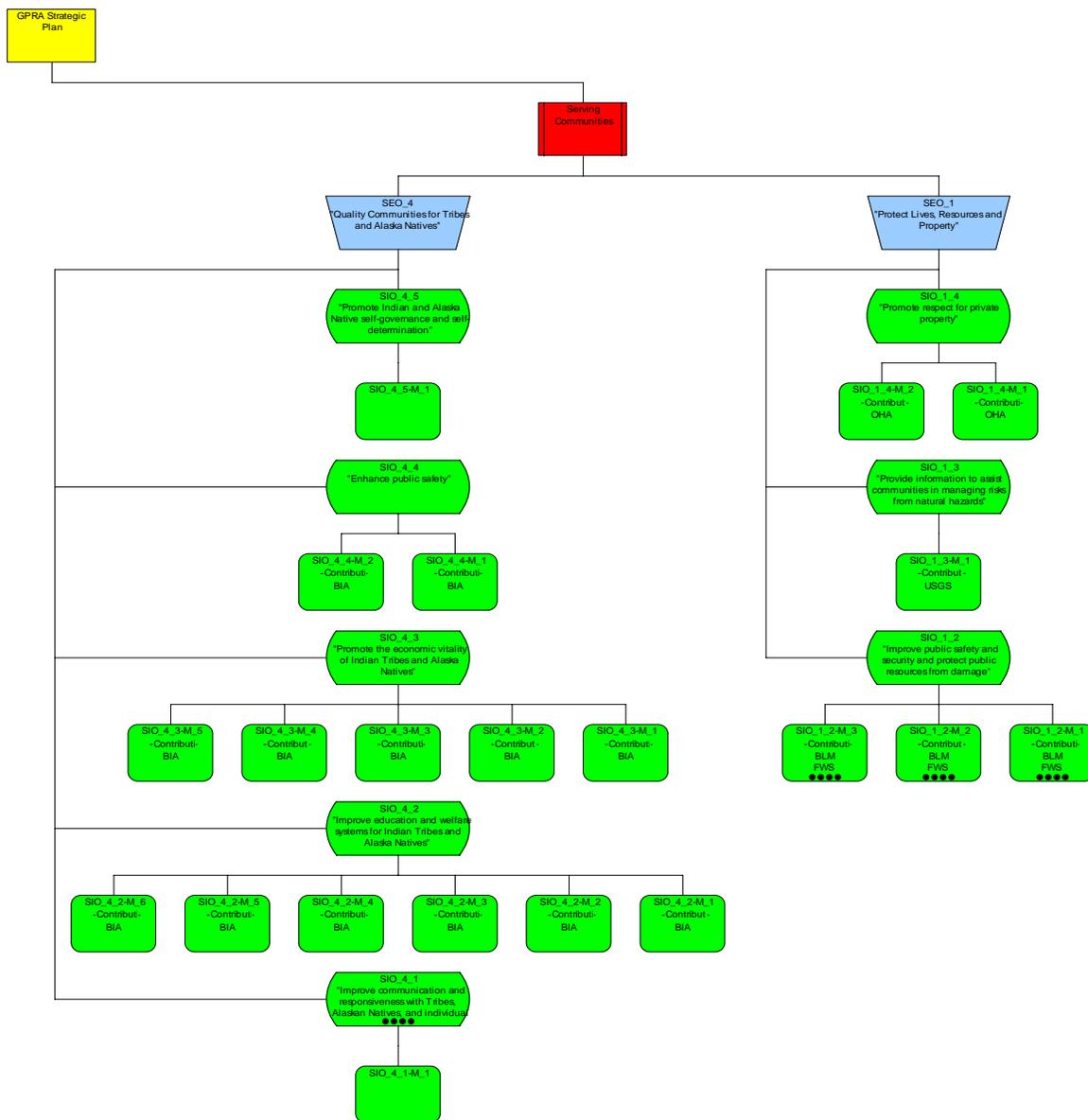


Figure 3-1. Law Enforcement Line of Business PRM Diagram

End Outcomes (EO) are long-term performance goals which describe and support the DOI’s strategic goals. End Outcomes express a desired result and are measured by one or more performance measures / indicators. Performance measures indicate the success in achieving the long-term goal. Intermediate Outcomes describe and support major milestones of an annual End Outcome goal. There are two or more Intermediate Outcome Goals to every End Outcome Goal. An examination of the PRM goals in Table 3-1 associated with the Law Enforcement LOB shows that support of a given goal varies across Bureaus. The Bureau of Indian Affairs has the greatest scope among Bureaus support the Law Enforcement LOB whereas the Bureau of Reclamation has the most limited Law Enforcement Scope.

**Table 3-1. Law Enforcement LOB End Outcomes mapped to Intermediate Outcomes**

End Outcome	End Outcome Description	Intermediate Outcome	Intermediate Outcome Description	Bureaus performing activities in support of goals
SEO_1	Protect lives, resources and property	SIO_1_3	Provide information to assist communities in managing risks from natural hazards	BIA BLM NPS FWS
		SIO_1_4	Promote respect for private property	BLM BOR FWS
		SIO_1_2	Improve public safety and security and protect public resources from damage	BIA BLM BOR NPS FWS
SEO_4	Advance quality communities for Tribes and Alaska Natives	SIO_4_1	Improve communication and responsiveness with Tribes, Alaskan Natives, and individual American Indians	BIA
		SIO_4_2	Improve education and welfare systems for Indian Tribes and Alaska Natives	BIA
		SIO_4_3	Promote the economic vitality of Indian Tribes and Alaska Natives	BIA
		SIO_4_4	Enhance public safety	BIA FWS (in Alaska)

End Outcome	End Outcome Description	Intermediate Outcome	Intermediate Outcome Description	Bureaus performing activities in support of goals
		SIO_4_5	Promote Indian and Alaska Native self-governance and self-determination	BIA

### 3.2 What functions does the Law Enforcement LOB perform?

Law Enforcement functions vary across DOI bureaus support the Law Enforcement LOB. Any proposed DOI-wide incident management and reporting system (e.g. IMARS) will need to support a wide variety of law enforcement functions which vary by Bureau. Table 3-2 is the description of Law Enforcement Functions by each bureau

**Table 3-2. Description of Law Enforcement Functions by DOI Bureau**

Bureau	Description of Law Enforcement Functions
Bureau of Land Management (BLM)	The BLM Law Enforcement Program is responsible for the detection, investigation, and enforcement of laws and regulations related to the use, occupancy, and development of the Public Lands. This includes resource protection and public safety. There are two types of BLM law enforcement officers, Rangers and Special Agents. Rangers are uniformed employees with responsibility to patrol public lands to deter, detect, investigate, and enforce resource protection laws and regulations. They also assist with search and rescue activities and coordinate with local, state, and federal land management and law enforcement agencies. The Special Agents are responsible for the investigation of all types of resource related crimes including cultural and natural resources, and mineral materials. There are approximately 250 total law enforcement officers in the BLM. The BLM has one IT system directly supporting their law enforcement activities – LAWNET.

Bureau	Description of Law Enforcement Functions
Bureau of Reclamation (BOR)	Bureau of Reclamation Law Enforcement activities are restricted to safe guarding the dams, powerplants, and canals under its control. BOR has constructed more than 600 dams and reservoirs including Hoover Dam on the Colorado River and Grand Coulee on the Columbia River. BOR is also the second largest producer of hydroelectric power in the western United States with 58 powerplants which must be safe guarded against potential threats. The BOR is currently using the FWS's LEMIS system to capture incident-related information. Plans call for the migration of the BOR incidents from LEMIS to IMARS.
Bureau of Indian Affairs (BIA)	The BIA's Law Enforcement mission is to uphold the constitutional sovereignty and customs of Tribes, while protecting the rights of all people; to protect life and property; ensure employment suitability and to promote and preserve peace within Indian country. The BIA's Law Enforcement responsibilities extend to over 170 reservations in 31 states. The BIA operates jails, performs patrolling activities on tribal lands, and performs investigations on tribal lands. The BIA Branch of Criminal Investigations has investigative responsibilities for crimes committed on, or involving, Indian country. This includes major federal crimes and state crimes assimilated into the Federal statues under Title 18 U.S.C. 1153. Indian Country jails incarcerate over 2000 individuals. The BIA processes as much as 12,000 individuals through their law enforcement system in a single month <sup>2</sup> . The BIA does not have any current BIA-wide IT systems supporting their law enforcement activities.
National Park Service (NPS)	The NPS's has Law Enforcement responsibilities for the 370 NPS sites across the United States and in Guam, Puerto Rico, and the Virgin Islands. There are approximately 1,500 full-time and 500 seasonal NPS Law Enforcement personnel. NPS law enforcement rangers patrol NPS lands; safe guard historic assets; respond to citizen reports of resource violations; issue citations, serves arrest warrants; participate in search and rescue; and sometimes coordinate activities with other local, state and federal land management and law enforcement agencies. The specific scope of NPS law enforcement varies from park to park. The NPS has two IT systems directly supporting their law enforcement activities: CIRS and CRIMES.

<sup>2</sup> <http://www.indianz.com/News/archives/002794.asp>

Bureau	Description of Law Enforcement Functions
Fish and Wildlife Service (FWS) Office of Law Enforcement (OLE)	FWS OLE efforts focus on threats to wildlife resource-illegal trade, unlawful commercial exploitation, habitat destruction, and environmental contaminants. The Law Enforcement Division of the FWS investigates wildlife crimes, regulates wildlife trade, and works in partnership with international, state, and tribal counterparts to conserve wildlife resources. Business functions include: Protecting wildlife from environmental hazards and safeguarding critical habitat for endangered species; protecting game species from illegal take and preserving legitimate hunting opportunities; inspecting wildlife shipments to ensure compliance with laws and treaties and detect illegal trade; working with international counterparts to combat illegal trafficking in protected species; and using forensic science to analyze evidence and solve wildlife crimes. The Division includes 252 special agents and 93 wildlife inspectors. The FWS has one IT system supporting their law enforcement and inspection activities: LEMIS
Fish and Wildlife Service (FWS) National Wildlife Refuge System (NWRS)	The FWS NWRS manages 545 refuges and 47 wetland management areas across the United States and in Guam, Puerto Rico, and the Virgin Islands. The refuge law enforcement program provides protection of trust species on and off Service lands as well as protection for natural and cultural resources, visitor protection, and protection of government property and employees. There are approximately 200 full-time and 200 dual function Law Enforcement personnel. NWRS law enforcement officers patrol Service lands; safe guard historic assets; respond to citizen reports of resource violations; issue citations, serves arrest warrants; participate in search and rescue; and sometimes coordinate activities with other local, state and federal land management and law enforcement agencies. The specific scope of law enforcement varies from refuge to refuge and may include easement violations. The FWS NWRS has one IT system supporting their law enforcement and inspection activities: LE-IMAGS. LE-IMAGS is a module under LEMIS and the two are treated as a single system.

The Department of the Interior’s (DOI) Integrated Business Reference Model (BRM) is an extension of the OMB’s FEAPMO Business Reference model. The BRM provides an organized, hierarchical construct for describing the day-to-day business operations of the Federal government. The DOI has extended its BRM beyond the Business Areas, Lines of Business, and Sub Functions defined by the FEA BRM Version 2.0 to the level of DOI function / activities which extend two to three levels beneath the FEA BRM. Figure 3-2 shows the BRM for the Law Enforcement LOB.

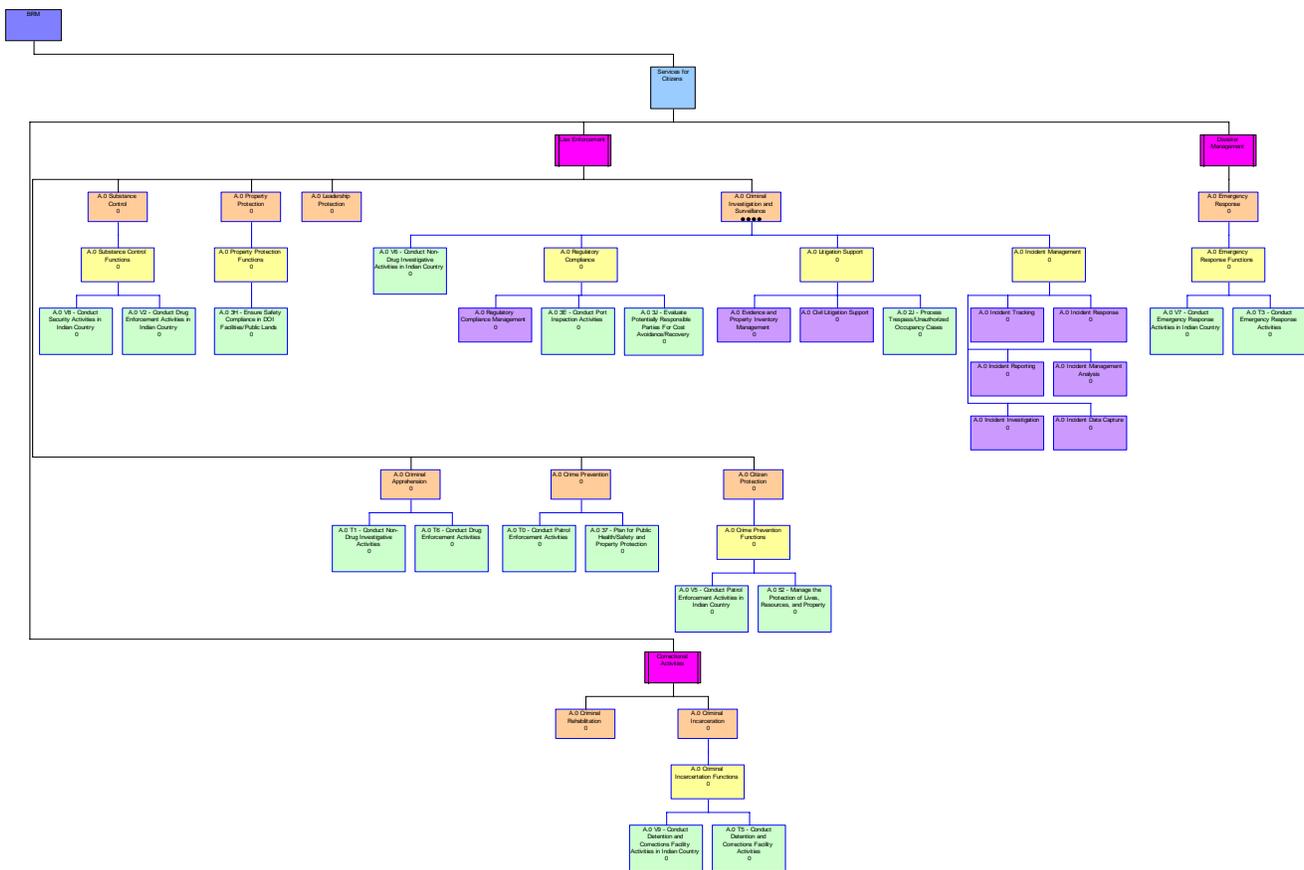


Figure 3-2. Law Enforcement Line of Business BRM Diagram

### 3.3 What IT Services are required by Law Enforcement?

The Service-Component Reference Model (SRM) provides a common technology neutral framework and vocabulary to characterize the IT and business components that collectively comprise an IT investment. The SRM helps the DOI with the development of modernization blueprints through the sharing and re-use of business and IT components. Investment-Projects can be directly associated with SRM Service Components, or the SRM Service Components may be derived from System associations. This section discusses the SRM service components that are relevant to the law enforcement LOB. Table 3-3 shows a comprehensive listing of SRM service components used by the law enforcement LOB.

Table 3-3. Law Enforcement LOB Service Components

Name	Description
Access Control	Defines the set of capabilities that support the management of permissions for logging onto a computer or network.
Ad Hoc	Defines the set of capabilities that support dynamic report creation.
Alerts and Notifications	Defines the set of capabilities that allow a customer to be contacted in relation to a subscription or service of interest.
Audio Conferencing	Defines the set of capabilities that support audio communications sessions among people who are geographically dispersed.
Audit Trail Capture and Analysis	Defines the set of capabilities that support the identification and monitoring of activities within an application or system.

Name	Description
CAD (Mapping Component of Computer Aided Design)	Defines the set of capabilities that supports the design, visualization, and mapping of objects using a computer.
Change Management	Defines the set of capabilities that control the process for updates or modifications to the existing documents, software or business processes of an organization.
Classification	Defines the set of capabilities that support selection and retrieval of records organized by shared characteristics in content or context.
Configuration Management	Defines the set of capabilities that control the hardware and software environments, as well as documents of an organization.
Content Authoring	Defines the capabilities that allow for the creation of tutorials, CBT courseware, Web sites, CD-ROMs and other interactive programs.
Content Review and Approval	Defines the capabilities that allow for the approval of interactive programs.
Data Classification	Defines the set of capabilities that allow the classification of data.
Data Cleansing	Defines the set of capabilities that support the removal of incorrect or unnecessary characters and data from a data source.
Data Exchange	Defines the set of capabilities that support the interchange of information between multiple systems or applications.
Data Integration	Defines the set of capabilities that support the organization of data from separate data sources into a single source using middleware or application integration and the modification of system data models to capture new information within a single system.
Data Mart	Defines the set of capabilities that support a subset of a data warehouse for a single department or function within an organization.
Data Recovery	Defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state.
Data Warehouse	Defines the set of capabilities that support the archiving and storage of large volumes of data.
Digital Signature	Defines the set of capabilities that guarantee the unaltered state of a file.
Document Imaging and OCR	Defines the set of capabilities that support the scanning of physical documents for use electronically.
Document Retirement	Defines the set of capabilities that support the termination or cancellation of documents and artifacts used by an organization and its stakeholders.
Email	Defines the set of capabilities that support the transmission of memos and messages over a network.
Encryption	Defines the set of capabilities that support the encoding of data for security purposes.
Extraction and Transformation	Defines the set of capabilities that support the manipulation and change of data.
Identification and Authentication	Defines the set of capabilities that support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.
Imagery	Defines the set of capabilities that support the creation of film or electronic images from pictures, paper forms or graphics for static or dynamic use.

Name	Description
Indexing	Defines the set of capabilities that support the rapid retrieval of documents through a structured numbering construct.
Information Retrieval	Defines the set of capabilities that allow access to data and information for use by an organization and its stakeholders.
Instrumentation and Testing	Defines the set of capabilities that support the validation of application or system capabilities and requirements.
Intrusion Detection	Defines the set of capabilities that support the detection of illegal entrance into a computer system.
Legacy Integration	Defines the set of capabilities that support the communication between newer generation hardware-software applications and the previous, major generation of hardware-software applications.
Library - Storage	Defines the set of capabilities that support document and data warehousing and archiving.
Loading and Archiving	Defines the set of capabilities that support the population of a data source with external data.
Mapping - Geospatial - Elevation - GPS	Defines the set of capabilities that support the use of elevation, latitude, and longitude coordinates.
Meta Data Management	Defines the set of capabilities that support the maintenance and administration of data that describes data.
Network Management	Defines the set of capabilities involved in monitoring and maintaining a communications network in order to diagnose problems, gather statistics and provide general usage.
OLAP	Defines the set of capabilities that support the analysis of information that has been summarized into multidimensional views and hierarchies.
Online Help	Defines the set of capabilities that provide an electronic interface to customer assistance.
Personalization	Defines the set of capabilities to change a user interface and how data is displayed.
Profile Management	Defines the set of capabilities that allow for the maintenance and modification of a customer's account information related to their profile.
Radiological	Defines the set of capabilities that support the use of radiation and x-ray technologies for analysis and scientific examination.
Real-Time - Chat	Defines the set of capabilities that support the conferencing capability between two or more users on a local area network or the internet.
Record Linking - Association	Defines the set of capabilities that support the correlation between logical data and information sets.
Requirements Management	Defines the set of capabilities for gathering, analyzing and fulfilling the needs and prerequisites of an organization's efforts.
Risk Management	Defines the set of capabilities that support the identification and probabilities or chances of hazards as they relate to a task, decision or long-term goal.
Role - Privilege Management	Defines the set of capabilities that support the granting of abilities to users or groups of users of a computer, application or network.
Shared Calendaring	Defines the set of capabilities that allow an entire team as well as individuals to view, add and modify each other's schedules, meetings and activities.

Name	Description
Software Development	Defines the set of capabilities that support the creation of both graphical and process application or system software.
Standardized - Canned	Defines the set of capabilities that support the use of pre-conceived or pre-written reports.
Subscriptions	Defines the set of capabilities that allow a customer to join a forum, listserv, or mailing list.
Surveys	Defines the set of capabilities that are used to collect useful information from an organization's customers.
Task Management	Defines the set of capabilities that support a specific undertaking or function assigned to an employee.
Threaded Discussions	Defines the set of capabilities that support the running log of remarks and opinions about a given topic or subject.
User Management	Defines the set of capabilities that support the administration of computer, application and network accounts within an organization.
Verification	Defines the set of capabilities that support the confirmation of authority to enter a computer system, application or network.
Video Conferencing	Defines the set of capabilities that support video communications sessions among people who are geographically dispersed.
Workgroup - Groupware	Defines the set of capabilities that support multiple users working on related tasks.

While the comprehensive list of FEA Service Components used by the Law Enforcement LOB is interesting, of perhaps greater relevance is the following table (Table 3-4) that shows existing Law Enforcement applications and the SRM Service Components used by each application.

**Table 3-4. Service Components mapped to Law Enforcement Applications**

System Acronym	System Name	SRM Service Component
CRIMES	Crime Reporting Incident Management Entry System	Access Control , Ad Hoc Reporting, Mapping - Geospatial - Elevation - GPS , Standardized-Canned Reporting, Information Retrieval, Verification
LAWNET	LAWNET Incident Reporting System	Access Control , Standardized-Canned Reporting, Data Exchange, Data Integration, Data Mart, Information Retrieval, Verification
LEMIS	Law Enforcement Information Management System	Access Control , Ad Hoc Reporting, Data Mart , Standardized-Canned Reporting, Information Retrieval, Verification
LE-IMAGS	Law Enforcement Information Management System NWRS Module (formerly known as LE-IMAGS)	Access Control , Ad Hoc Reporting, Data Mart , Mapping - Geospatial - Elevation – GPS, Standardized-Canned Reporting, Information Retrieval, Verification
CIRS	Case Incident Reporting System	Access Control, Standardized-Canned Reporting, Information Retrieval, Verification

From a service component view, the systems are similar. They are all essentially access-controlled data collection, storage, retrieval, and visualization applications. There is a need to exchange information with other systems (e.g. NIBRS) and to tailor output to given user groups. Security and user authentication is important as information is sensitive and different users and user groups should only have access to information that is relevant to their case. In some cases, on-going investigations and special operations may contain especially sensitive data. The SRM analysis supports the notion that a single system (IMARS) will be able to replace the services provided by the existing systems. The proposed IMARS system must have flexible reporting and information retrieval features.

## 4. Findings and Recommendations

### 4.1 Program Findings & Recommendations

Program findings refer to general issues concerning, funding, planning, workforce, objectives, or communication and outreach

**Program Finding 1** - *Current Law Enforcement Systems provide similar functions and services and are isolated along organizational boundaries. These redundancies and inefficiencies are being addressed by the planned Departmental IMARS procurement planned for early Fiscal Year 2005.*

An examination of current law enforcement systems in Table 4-1 shows similar functions and services isolated along organizational boundaries.

**Table 4-1. Service Components mapped to Law Enforcement Applications**

System Acronym	System Name	SRM Service Component
CRIMES	Crime Reporting Incident Management Entry System	Access Control , Ad Hoc Reporting, Mapping - Geospatial - Elevation - GPS , Standardized-Canned Reporting, Information Retrieval, Verification
LAWNET	LAWNET Incident Reporting System	Access Control , Standardized-Canned Reporting, Data Exchange, Data Integration, Data Mart, Information Retrieval, Verification
LEMIS	Law Enforcement Information Management System	Access Control , Ad Hoc Reporting, Data Mart , Standardized-Canned Reporting, Information Retrieval, Verification
LE-IMAGS	Law Enforcement Information Management System NWRS Module (formerly known as LE-IMAGS)	Access Control , Ad Hoc Reporting, Data Mart , Mapping - Geospatial - Elevation – GPS, Standardized-Canned Reporting, Information Retrieval, Verification
CIRS	Case Incident Reporting System	Access Control, Standardized-Canned Reporting, Information Retrieval, Verification

At the time of this report, the DOI was in the process of procuring the IMARS system. The Incident Management Analysis and Reporting System (IMARS) is being procured to provide a Department-wide information collection, analysis, and reporting system for information from three inter-related activities. These activities are law enforcement, emergency management, and security.

IMARS will be an automated system that will allow law enforcement (including emergency management and security) areas within DOI to identify, collect, store, retrieve, analyze, manage and report information related to incidents. IMARS will allow DOI and bureau personnel to create reports in various formats, sort data, conduct data analysis and interface with other systems, both within DOI and outside of it. IMARS will give DOI an enhanced ability to:

- Capture, integrate and share law enforcement and related information from other sources
- Identify needs (training, resources, etc.)
- Measure performance of law enforcement programs, management of emergency incidents
- Meet reporting requirements
- Analyze and prioritize protection efforts

- Justify requests and expenditures
- Manage visitor use and protection programs
- Prevent, detect and investigate criminal activity
- Protect natural and cultural resources

An examination of the common business function supported by current systems shows significant commonality which supports the contention that a single Department-wide system (IMARS) will be able to meet the majority of Bureau and Departmental business needs.

Table 4-2 below shows a comparison of planned IMARS and current Bureau LE System functionality. It can be seen that planned IMARS functionality will encompass the wide range of functionality currently provided by the Bureau-specific solutions.

**Table 4-2. Comparison of IMARS and Bureau LE System Functionality**

System	Bureau	Incident Data Collection / Reporting	NIBRS-Compliant Reporting	Case Management	Advanced Queries	Geospatial	Computer Aided Dispatch	Legal Case Research	Asset Management	Time Recording
IMARS	BLM, BIA, BOR, NPS, FWS	X	X	X	X	X	X	FWS only	Maximo or FBMS	FBMS
CRIMES	NPS	X			Simple Queries					
LAWNET	BLM	X	X	X	Simple Queries					X
LEMIS	FWS	X		X	X			X	X	
LEMIS – NWRS	NWRS	X			X					
CIRS	NPS	X			Simple Queries					

**Program Finding 2** - *LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report; however LAWNET does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, report crime statistics to the DOJ/FBI through the Department.*

Currently law enforcement authorities are required to aggregate the number of incidents by offense type monthly and report these totals to the FBI. The FBI's Uniform Crime Reporting (UCR) program, which began in 1929, collects information about crimes reported to the police. The FBI's National Incident-Based Reporting System (NIBRS) collects data on crime incidents in support of the UCR Program. Under incident-based reporting, agencies provide an individual record for each crime reported.

Currently only the BLM's LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report. LAWNET, however, does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, reports crime statistics to the DOJ/FBI through the Department. Since the Department of Interior has yet to switch to NIBRS from the UCR format of reporting, the BLM is reporting crime statistics in the UCR format even though it is NIBRS compliant. The UCR is submitted once a year around March and includes crime statistics for the previous calendar.

The proposed IMARS system is designed to support uniform incident collection and reporting across all Bureaus in support of these metrics. IMARS will facilitate NIBRS compliance. It is recommended that the DOI Proceed with procurement of Enterprise Incident Management System using collaborative approach and retire four existing systems at NPS (CRIMES, CIRS), BLM (LAWNET) and FWS

(LEMIS Non-core) in a timely fashion to facilitate uniform collection of crime statistics to the FBI’s NIBRS system in support of the UCR Program across the DOI.

## 4.2 System Findings & Recommendations

System findings refer to findings concerning the relative maturity of the deployed IT systems and how well they support the LOB mission.

**System Finding 1** - *Current Law Enforcement Systems support similar primary business functions.*

An examination of current law enforcement systems in Table 4-3 shows multiple Bureau systems supporting similar law enforcement business functions.

**Table 4-3. Comparison of DOI Law Enforcement Systems**

System Acronym	System Architecture	Development Language	Data Model	Primary Function(s)
CRIMES	Fat Client (stand alone MS Access databases)	Visual Basic	No	Incident data collection and reporting. NIBRS compliant.
LAWNET	Client-Server	Clipper, SQL	Yes	Incident data collection, reporting, and queries. Time reporting, incident queries, case management,
LEMIS	Web-based (requires dedicated connection to server)	Java, Java Script, Cold Fusion, HTML	No	Incident data collection, reporting, queries, case management, case law research, declarations, asset management
LE-IMAGS	Web-based (requires dedicated connection to server)	Java, Java Script, HTML, JBOSS	No	Incident data collection, reporting, case management, and easement violations. Some simple geospatial functionality for collection of location data using map interface.
CIRS	Fat Client (stand alone DOS-based databases)	Clipper	No	Incident data collection and reporting. NIBRS compliant.

The commonality of business functions among examined law enforcement systems supports the hypothesis that a single system (IMARS) could meet 80% or more of the required functionality across all business units. The FWS (LEMIS) is one exception with customs declarations and case law research that will not be addressed by the IMARS procurement.

**System Finding 2** - *Current Law Enforcement Systems are not integrated and have deployed non-shared, Bureau-system-specific infrastructure investments.*

Currently it is not possible to query for incidents across multiple NPS parks or across multiple DOI Bureaus. Given the fact that each system was developed independently with different technologies and database schemas, it is not currently possible to consolidate the data for cross departmental analyses or reporting. Any DOI-wide analyses or cross Bureau analyses must be done manually. Table 4-4 shows existing Law Enforcement System along with their general descriptions. Figure 4-1 provides conceptual system architecture of the existing systems.

**Table 4-4. Law Enforcement System Descriptions**

System Acronym	System Name	System Owner	General System Description
CRIMES	Crime Reporting Incident Management Entry System	NPS	<p>The CRIMES application was developed to meet a tactical need for a single National Park and was then adopted by upwards of 100 parks within the NPS. User requirements are addressed in an ad hoc fashion by the sole system developer, Peter Paul. System downloads are posted at <a href="http://www.mora.nps.gov/crimes">www.mora.nps.gov/crimes</a>. There is no formal help desk or problem tracking system supporting the CRIMES application. Functionally, CRIMES is redundant to the CIRS incident reporting system still used by the NPS, but unlike CIRS, CRIMES is not NIBRS compliant. CRIMES is an MS Access 97 database with a Visual Basic user interface. Some larger NPS parks are reaching the 1GB Access database limitation with four years of collected data. CRIMES databases only encompass a single park, there is no centralized CRIMES database that goes across multiple parks.</p>
LAWNET	LAWNET Incident Reporting System	BLM	<p>LAWNET is a BLM-developed incident tracking and reporting system. LAWNET was designed and developed in 1994 – 1997 and went in to operation in October, 1997. Currently more than 117,000 Law Enforcements incidents have been entered in to the system. The expected life cycle of the LAWNET application was 3 to 5 years. LAWNET has exceeded this life cycle. LAWNET was designed around a store and forward architecture (client/server) so users can take their notebook computers into the field and enter the data. When users return to their offices, they connect the computer to the network and upload incidents to the LAWNET central server. LAWNET features time and charge code fields to track how much time a user spends working a specific incident. LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report, however LAWNET does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, report crime statistics to the DOJ/FBI through the Department. Since the Department of Interior has yet to switch to NIBRS from UCR format of reporting, the BLM is reporting crime statistics in the UCR format even though it is NIBRS compliant. The UCR is submitted once a year around March and includes crime statistics for the previous calendar year. LAWNET is a DOS-based system that is based on Clipper 5.3 with a centralized SQL Informix database located the National Interagency Fire Center in Boise, ID. Users of LAWNET complain of excessive access / download times. While LAWNET data is structured and defined, ad hoc queries are difficult and reporting is very limited. LAWNET has formal training and a well defined support infrastructure.</p>

System Acronym	System Name	System Owner	General System Description
LEMIS	Law Enforcement Information Management System	FWS	LEMIS is an n-tier client/server web application written in Cold Fusion. It features a thin client (web browser) and a MS SQL Server 2000 database. It uses Cold Fusion and Java Script. It does not comply with the Active Directory access control model being adopted by the DOI, but will in December, 2004. LEMIS also has an incident management module used by NWRS called IMARS/FWS/RLE. IMARS/FWS/RLE is a J2EE-compliant module and currently uses JBOSS (an open source J2EE application server and development environment similar to Cold Fusion). IMARS/FWS/RLE does comply with the Active Directory access control model. Sharing of components between LEMIS and the IMARS/FWS/RLE module will occur at the database layer using Java data objects and/or Cold Fusion.
CIRS	Case Incident Reporting System	NPS	CIRS is a NIBRS compliant incident collection and reporting system in use by the NPS at 40 to 50 national parks. CIRS is a DOS (Clipper) application, but unlike the BLM's LAWNET system, CIRS does not have a centralized database.

It is recommended that the DOI procure the IMARS system and implement a single incident management system across the DOI. Given the significant investment in LEMIS and significant variations on the law enforcement business functions performed by the FWS, the FWS may elect to maintain and use their LEMIS as a front-end client to the DOI-wide IMARS repository.

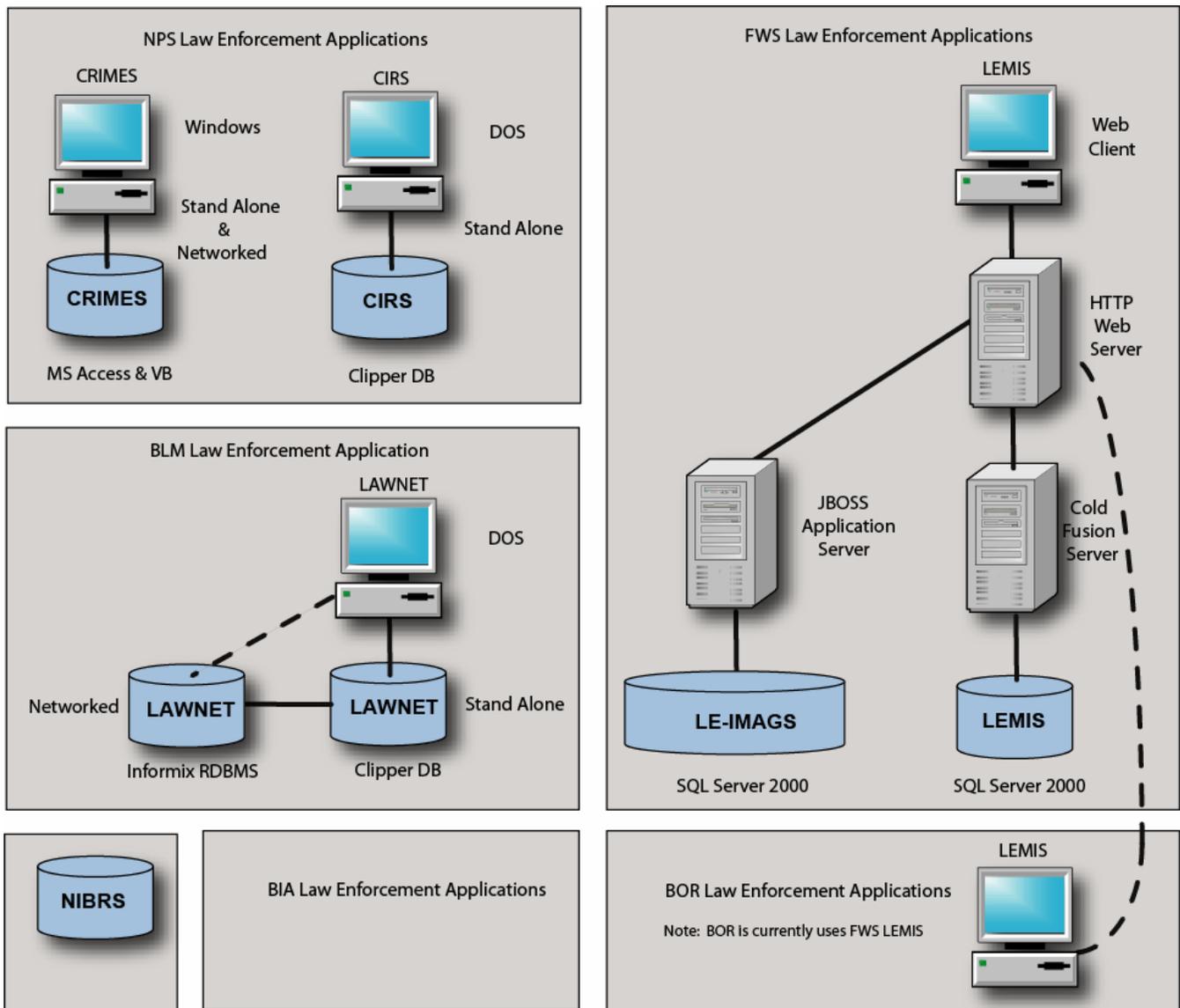


Figure 4-1. Current Law Enforcement System Architecture

**System Finding 3 - Current Law Enforcement Systems provide similar services.**

As part of the Law Enforcement LOB analyses, systems were examined and described in terms of the SRM services they provided or utilized. From a service component view, the systems are similar. They are all essentially access-controlled data collection, storage, and retrieval applications. There is a need to exchange information with other systems (e.g. NIBRS) and to tailor output to given user groups. Security and user authentication is important as information is sensitive and different users and user groups should only have access to information that is relevant to their case. In some cases, on-going investigations and special operations may contain especially sensitive data. The SRM analysis supports the notion that a single system (IMARS) will be able to replace the services provided by the existing systems. Table 4-5 depicts the service components mapped to the Law Enforcement Applications.

**Table 4-5. Service Components mapped to Law Enforcement Applications**

System Acronym	System Name	SRM Service Component
CRIMES	Crime Reporting Incident Management Entry System	Access Control , Ad Hoc Reporting, Mapping - Geospatial - Elevation - GPS , Standardized-Canned Reporting, Information Retrieval, Verification
LAWNET	LAWNET Incident Reporting System	Access Control , Standardized-Canned Reporting, Data Exchange, Data Integration, Data Mart, Information Retrieval, Verification
LEMIS	Law Enforcement Information Management System	Access Control , Ad Hoc Reporting, Data Mart , Standardized-Canned Reporting, Information Retrieval, Verification
LE-IMAGS	Law Enforcement Information Management System NWRS Module (formerly known as LE-IMAGS)	Access Control , Ad Hoc Reporting, Data Mart , Mapping - Geospatial - Elevation – GPS, Standardized-Canned Reporting, Information Retrieval, Verification
CIRS	Case Incident Reporting System	Access Control, Standardized-Canned Reporting, Information Retrieval, Verification

### 4.3 Business Findings & Recommendations

Business findings refer to the findings concerning functional activities or process findings that would facilitate improvements to the LOB.

**Business Finding 1** - *Activities performed by Bureaus supporting the law enforcement LOB vary across the DOI, but there are core function activities that are suitable for cross departmental automation.*

Table 4-4 shows the BRM function / activities as performed by each Bureau with indications of whether or not these functions are automated. The table is color coded with red signifying a manually performed function / activity, yellow signifying a function / activity that is supported in a limited fashion by an existing IT system, and green signifying a function / activity that is fully supported by an existing IT system. An examination of Table 4-6 shows that law enforcement incident management and reporting is largely non-automated. Table 4-6 goes on to show that systems operated the FWS are currently the most mature in terms of automation. The BIA and BOR have no automated systems supporting law enforcement activities. The BLM’s level of automation is below that of the FWS but ahead of the NPS which uses two separate systems that provide limited point solutions on a park-by-park basis.

Current systems such as the BLM’s LAWNET are after-the-fact data collection systems which do not support field-based law enforcement activities. Field personnel must collect incident data manually and then re-enter the data into LAWNET upon their return from the field. Because of the lack of automation, incident information collection is currently an added burden to law enforcement personnel. The BLM’s LAWNET system requires field personnel to re-key incident data collected by hand in the field into the LAWNET system after-the-fact. No support is provided in the field where law enforcement personnel spend the majority of their time.

**Table 4-6. Level of Automation of Law Enforcement Functions by DOI Bureau**

Function / Activity	BIA	BLM	BOR	FWS	NPS
3E - Conduct Port Inspection Activities				X	
Civil Litigation Support	X	X		X	X
Evidence and Property Inventory Management	X	X		X	X
Incident Data Capture	X	X	X	X	X
Incident Investigation	X	X	X	X	X
Incident Management Analysis	X	X	X	X	X
Incident Reporting	X	X	X	X	X
Incident Response	X	X	X	X	X
Incident Tracking	X	X	X	X	X
Regulatory Compliance Management	X	X	X	X	X
T0 - Conduct Patrol Enforcement Activities	X	X		X	X
T1 - Conduct Non-Drug Investigative Activities	X	X		X	X
T6 - Conduct Drug Enforcement Activities	X	X			X
V2 - Conduct Drug Enforcement Activities in Indian Country	X				
V5 - Conduct Patrol Enforcement Activities in Indian Country	X				
V5 - Conduct Patrol Enforcement Activities in Indian Country	X				
V6 - Conduct Non-Drug Investigative Activities in Indian Country	X				
V8 - Conduct Security Activities in Indian Country	X				
V7 - Conduct Emergency Response Activities in Indian Country	X				
T3 - Conduct Emergency Response Activities	X	X			X
V9 - Conduct Detention and Corrections Facility Activities in Indian Country	X				
T5 - Conduct Detention and Corrections Facility Activities					

An examination of Table 4-6 shows the BIA’s functions are the most wide-reaching of all DOI bureaus. The BIA’s Law Enforcement responsibilities extend to over 170 reservations in 31 states. The BIA operates jails, performs patrolling activities on tribal lands, and performs investigations on tribal lands. Of the 74 detention facilities in Indian country in the West, the BIA directly operates 19 and provides funding for operation of 46 others, and nine others are operated by tribes with their own funds. Currently, the BIA appears to have no enterprise applications for the management of their detention facilities. The IMARS system must be robust enough to capture BIA-specific detention center-related incidents but the procurement of a DOI-wide detention facility system automation application is likely outside the scope of the IMARS procurement and is not recommended. Fortunately, there are numerous COTS software applications that automate common detention and corrections facilities activities. These software systems should be examined for their compatibility with the proposed IMARS procurement.

**Business Finding 2** – *The planned IMARS procurement will provide a level of automation for core business functions across all Bureaus supporting the law enforcement LOB.*

An examination of Table 4-7 shows a significant amount of commonality of law enforcement functions performed across all Bureaus supporting the DOI law enforcement LOB. It should be noted that while law enforcement functions appear to be similar when viewed a high-level of abstraction, the scope and functions that make up law enforcement varies across Bureaus. Forms used by Bureaus differ, data collected differ, and the codes (CFR) that govern Bureau law enforcement activities vary from Bureau to Bureau. Any proposed law enforcement system will need to support a wide-range of forms, legal codes, and functions that will likely vary Bureau-by-Bureau. Table 4-7 shows the most common function activities across all Bureaus within the law enforcement LOB. The functions were ranked in terms of their current level of automation and criticality. The only function activity that may not be a good candidate for inclusion within IMARS would be the civil litigation support as these requirements may vary significantly by Bureau and there currently exists a sufficient capability with FWS’s LEMIS application. The functions highlighted in red are those which are currently unsupported by automation yet have commonality across the Bureaus and have mission criticality.

**Table 4-7. Current Level of Automation and Mission Criticality of Law Enforcement Functions**

<b>Function / Activity</b>	<b>Function / Activity Description</b>	<b>Current Level of Automation</b>	<b>Criticality</b>
Civil Litigation Support	This activity supports the management and coordination of the law enforcement resources required by the court to process a legal action. - Derived from IMARS Needs Assessment Civil Litigation Support	Medium	Medium
Evidence and Property Inventory Management	This activity support the management requirements for legal evidence and property management in support of litigation - Derived from IMARS Needs Assessment Evidence and Property Inventory Management	Low	Medium
Incident Data Capture	This activity describes capturing all the initial information required to document an identified incident. - Derived from IMARS Needs Assessment Incident Data Capture	Medium	Medium
Incident Investigation	Incident investigation is the activity where the requisite skills are assigned to conduct a complete investigation. The investigation provides additional information to support the lifecycle of the incident. The incident status is generated from the ongoing investigative work. - Derived from IMARS Needs Assessment Incident Investigation	Low / Medium	High
Incident Management Analysis	This activity provides support for the analytical techniques and approaches to mining the incident reporting and other law enforcement databases for historical trends and patterns. This information can be used for assessing the level and type of resource use, vulnerabilities trends and patterns as well as any other aspect of the incident process. - Derived from IMARS Needs Assessment Incident Management Analysis	Low	Medium
Incident Reporting	This is the general practice to report on the information captured during the initial incident data capture and ongoing investigation to provide summary and detailed reports. Examples of these reports could range from status of investigations or current allocation of resources. This type of reporting is operational in nature. - Derived from IMARS Needs Assessment Incident Reporting	Medium	Medium

Function / Activity	Function / Activity Description	Current Level of Automation	Criticality
Incident Response	Incident response is the action of applying investigative resources and responding to the identified incident. - Derived from IMARS Needs Assessment Incident Response	Low	High
Incident Tracking	Incident Tracking establishes the information required to manage the lifecycle of the incident. This information provides the ability for law enforcement management to - Derived from IMARS Needs Assessment Incident Tracking	Low	Medium
Regulatory Compliance Management	This is the general practice to report on the information captured during the initial incident data capture and ongoing investigation to provide compliance with federal requirements established to manage specific types of incidents. Examples would include ARPA, EPA NIBRS, NHTSA and DOT types of mandatory reporting. This activity fulfills the federal reporting requirement. that - Derived from IMARS Needs Assessment Regulatory Compliance Management	Low	Medium
T0 - Conduct Patrol Enforcement Activities	The purpose of conducting patrol and enforcement activities is to prevent, deter, and apprehend those involved in unlawful activity. These activities provide a safe environment for visitors, residents, and employees and protect natural resources, critical infrastructure, and other facilities within the Department's responsibilities. Patrol and enforcement activities include:	Low	High
T1 - Conduct Non-Drug Investigative Activities	The purpose of conducting non-drug enforcement investigative activities is to produce a factual report so appropriate authorities can determine a suitable course of action. Investigative activities include: Grand jury: interviews, prepare/serve subpoenas, testify; coordinate with prosecutors prior to filing charges.	Low	High
T6 - Conduct Drug Enforcement Activities	Drug enforcement activities include marijuana cultivation, methamphetamine production and cross-border smuggling, all causing the destruction of natural resources and increasing the risk to safety of public employees. Such activities should be primarily drug related and/or of such significance that it is the primary reason for the activity. Other enforcement activities, where drugs are of secondary significance (e.g. traffic stop for moving violations nets a simple possession charge for marijuana) should be considered a patrol activity.	Low	High

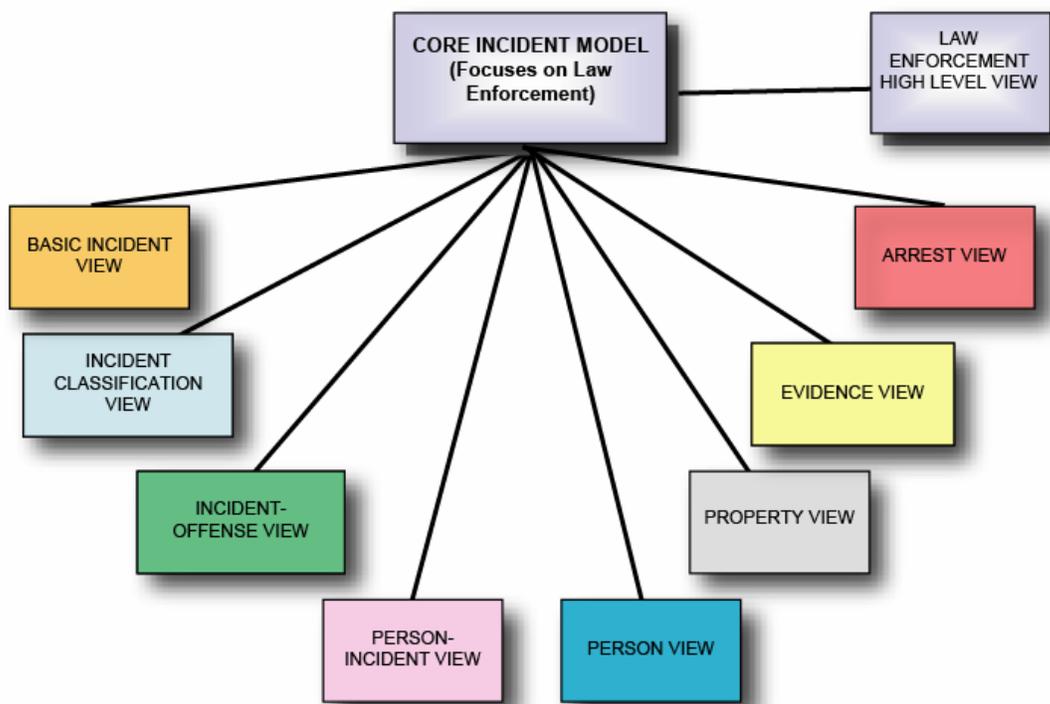
The current IMARS strategy of implementing a records management system in tandem with a computer-aided dispatch system appears to be in alignment with the above recommendations. The records management and computer-aided dispatch system address the function / activities highlighted in red in table 4-5.

#### 4.4 Data Findings & Recommendations

Data findings refer to the findings identifying opportunities for data sharing or data exploitation to improve business intelligence or efficiency.

**Data Finding 1** - *There is clearly a need for a DOI-wide law enforcement data model. Physical data models of existing systems and a conceptual data model of the planned IMARS system will be necessary to effectively plan any data migration and/or system integration.*

There is clearly a need for a DOI-wide law enforcement data model. Some initial efforts have been made in this area (see the Law Enforcement Data Subject Areas in Figure 4-2), but both a ‘to be’ conceptual data model and ‘as is’ data models much be collected in a uniform manner across all DOI law enforcement systems that will have data migrated to the planned IMARS system.



**Figure 4-2. Law Enforcement Data Subject Areas**

Physical data models for existing Bureau incident management systems are largely non-existent. Some Bureaus expressed the need to migrate existing data to any proposed system. The NPS has indicated plans for migration of some CIRS data to IMARS pending an initial feasibility study. Physical data models of existing systems and a conceptual data model of the planned system will be necessary to effectively plan any data migration.

The current IMARS functional requirements document does not adequately address data migration from current bureau applications to IMARS. The business case does briefly mention that LEMIS and IMARS will be integrated, but provides limited details on how this integration will be performed. Interviews with CRIMES, CIRS, LAWNET, and LEMIS system owners and users indicate a belief that existing incident data and historical data will be migrated to the proposed IMARS system. The LAWNET business case specifically states, “all existing LAWNET data will be converted into this [IMARS] system”. It is recommended that a comprehensive data migration plan be developed as part of the IMARS procurement.

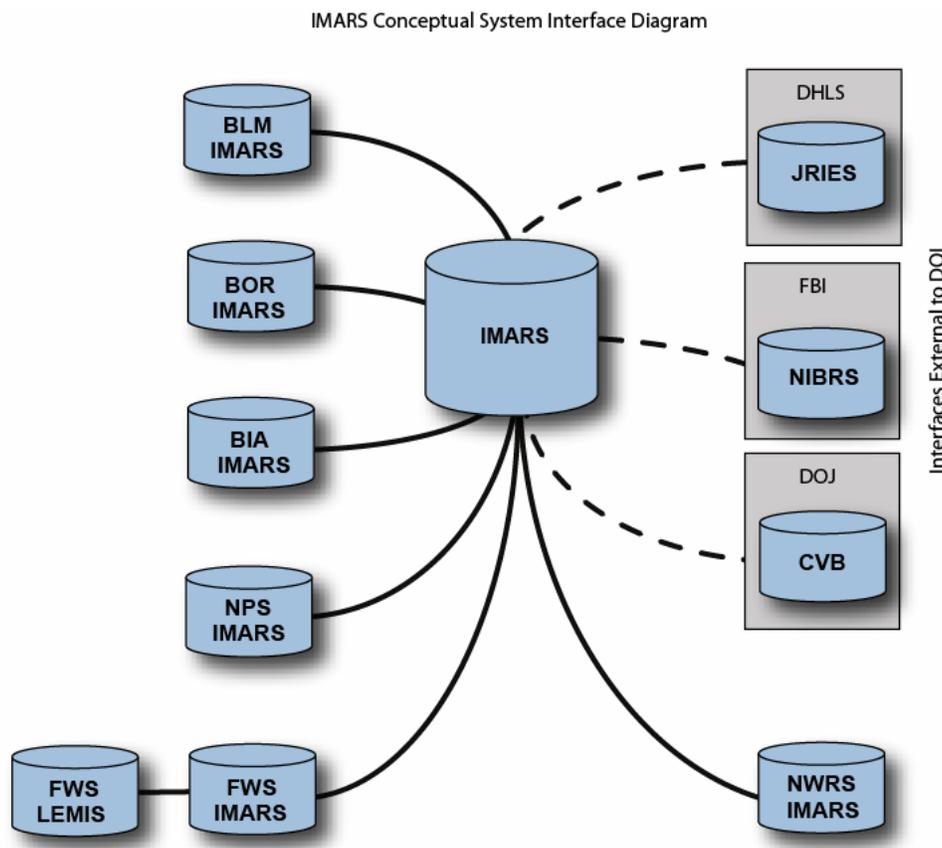
In addition, there is a need to share law enforcement data across Federal, State, and Local law enforcement agencies. The IMARS development team should investigate the following initiatives for possible inclusion in a DOI-wide enterprise data model for the law enforcement LOB.

- The Automatic Crash Notification (CAN) Initiative.
- Common Alerting Protocol (CAP)
- Critical Infrastructure Protection Initiative (CIPI)

- Emergency XML (EM-XML) Consortium
- IEEE Incident Management Working Group (IMWG) – (Responsible for IEEE 1512-2000, *Standard for Common Incident Management Message Sets for use by Emergency Management Centers.*)
- IETF Incident Object Description and Exchange Format (IODEF)
- IEF Intrusion Detection Exchange Format (IDMEF)
- OASIS Emergency Management Technical Committee
- OpenSec Advisory and Notification Markup Language (ANML)
- Standard for Encoding, Exchanging, and Storing Public Safety Data – National Institute of Justice, Ver. 2.21: 2003
- National Criminal Information Center, FBI CJIS
- Justice and Public Safety XML Data Dictionary Schema – USDOJ OJP ISWG.

**Data Finding 2** - *The planned IMARS system has extensive requirements for interfacing with existing DOI, Bureau, and external systems that span law enforcement, facilities management, asset management, and accounting. These interface requirements highlight the need for a published IMARS data model and DOI-wide standards for information exchanges between these systems.*

Conceptually, the IMARS architecture calls for a central DOI IMARS repository with Bureau-specific instantiations of IMARS. The one exception being the FWS which will have both a FWS instantiation and an instantiation for its NWRS organization. IMARS has external system interfaces to the FBI, DHLS, and DOJ systems. These high-level conceptual system interfaces are shown in the Figure 4-3 below.



**Figure 4-3. IMARS Conceptual System Interface Diagram**

Table 4-8 details the interface requirements between the central IMARS server and its external interfaces. It is recommended that during the implementation of IMARS the exact nature of the interface, the information exchange mechanism, and the frequency of updates / information exchanges be thoroughly documented.

**Table 4-8. IMARS Central Server System Interfaces**

IMARS Module	System Interface	Nature of Interface <sup>3</sup>
IMARS (Central DOI Server)	FBI National Incident-Based Reporting System (NIBRS).	IMARS shall provide a means to extract NIBRS data and transfer it to the FBI from within the program. <a href="http://www.fbi.gov/ucr/ucr.htm#nibrs">http://www.fbi.gov/ucr/ucr.htm#nibrs</a>
	Central Violations Bureau (CVB).	IMARS shall be able to accept import of data from the CVB when that data is delivered in the standard interface format. A log file shall track the success or failure of each attempted CVB update to the IMARS central server data. <a href="http://www.uscourts.gov/ttb/aug03ttb/violations/index.html">http://www.uscourts.gov/ttb/aug03ttb/violations/index.html</a>
	Department of Homeland Security Joint Regional Information Exchange System (JRIES).	JRIES is a counterterrorism communications program founded and managed in conjunction with state and local governments, counterterrorism authorities, and law enforcement agencies. This platform has been adopted by Homeland Security as the system of choice for information sharing between DHS partners as part of the Homeland Security Information Network. JRIES provides real-time collaboration and advanced analytic capabilities. The exact nature of IMARS and JRIES information exchange is TBD. <a href="http://www.dhs.gov/dhspublic/display?theme=35&amp;content=3348&amp;print=true">http://www.dhs.gov/dhspublic/display?theme=35&amp;content=3348&amp;print=true</a>
	Personal Digital Assistants (PDAs)	The IMARS system shall provide the ability to download data into Personal Digital Assistants (PDAs). There is no standard PDA operating system across the DOI, so IMARS will need to support Windows Mobile and Palm OS.

#### 4.4.1 NPS Specific IMARS Interface Requirements

IMARS will initially be implemented as a pilot program that will be accessible to seven NPS park sites. Once the pilot sites are implemented, the pilot site personnel will use the system for 90 days. The successful completion of the pilot phase will initiate the roll out of IMARS to all NPS parks and will initiate pilot phases for other DOI bureaus. It should be noted that the final IMARS product will be customized somewhat for individual Bureau needs. Pending funding and staff availability individual Bureaus may elect to pilot the IMARS software. BLM is prepared and has requested the opportunity to pilot IMARS concurrently with the National Park Service.

The National Park Service IMARS interfaces are the most extensive among the DOI bureaus. The interface requirements gathered from IMARS procurement documentation shows upwards of 15 different system interfaces. The NPS also has requirements for web browser, mobile computing, PDA, radio / pager, and cellular device connectivity. These conceptual system interfaces are shown in Figure 4-4 below.

<sup>3</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.

IMARS NPS Detailed Conceptual System Interface Diagram

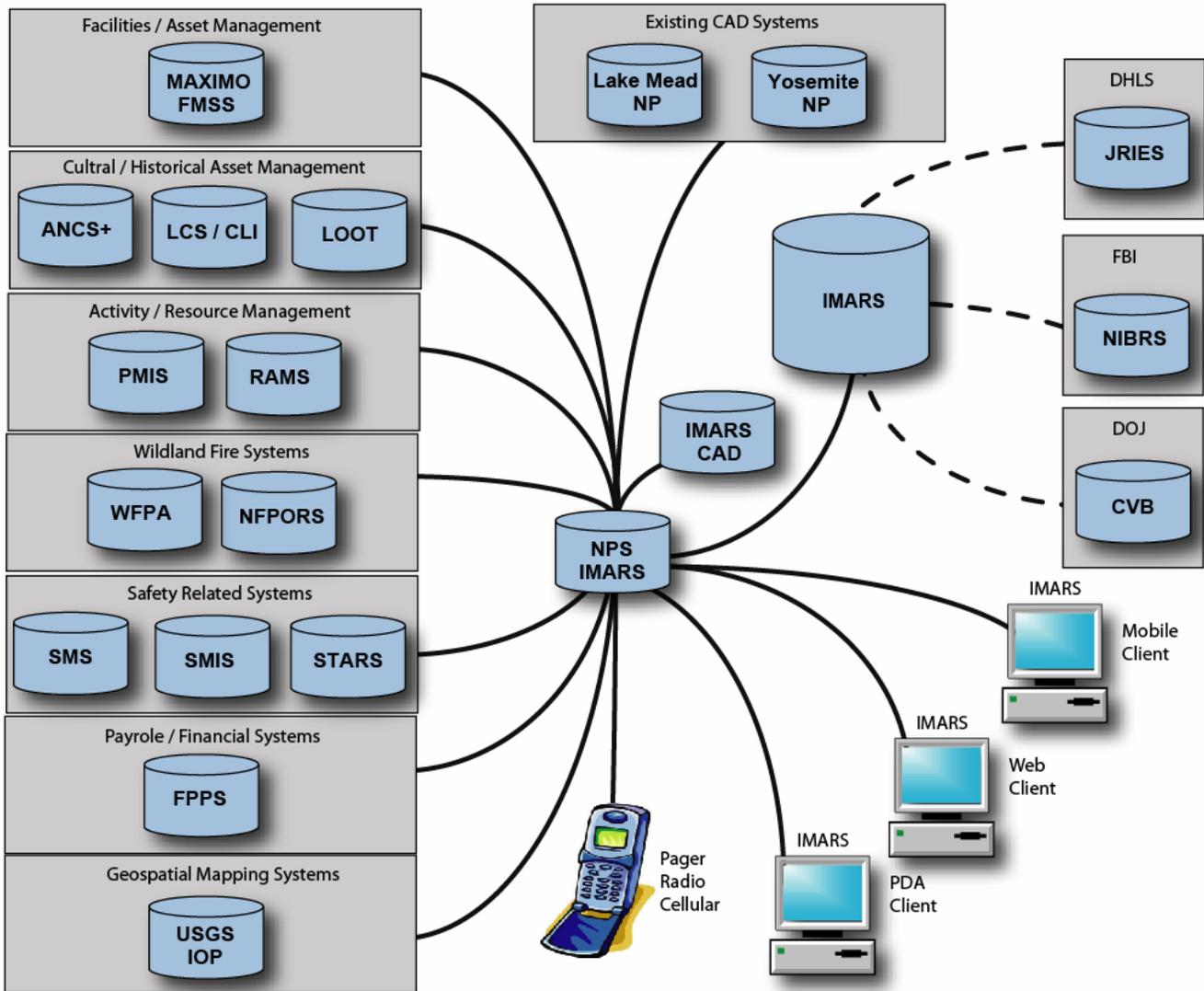


Figure 4-4. IMARS NPS Detailed System Interface Diagram

Table 4-9 details the interface requirements between the NPS IMARS server and its Bureau, Departmental, and external interfaces. The extensive number and variety of interfaces highlights the need for information exchange and data warehousing techniques to facilitate information exchange between these systems. The DOI TRM recommend the use of W3C Simple Object Access Protocol (SOAP) or American National Standards Institute X12 Electronic Data Exchange (ANSI X12 EDI) and the variety of interfaces as preferred standards to implement information exchange. In viewing the following table, it can be seen that the exact nature of certain system interfaces are TBD (to be determined). Vague system interface requirements may introduce implementation / schedule risk to the IMARS program unless adequately addressed. It is recommended that during the implementation NPS IMARS pilot, the exact nature of the interface, the information exchange mechanism, and the frequency of updates / information exchanges be thoroughly documented.

**Table 4-9. IMARS NPS System Interfaces**

IMARS Module	System Interface	Nature of Interface <sup>4</sup>
IMARS NPS	Facility Management Software System (FMSS)/MAXIMO	The system shall provide the capability to interface with the FMSS for importing, exporting, and reporting on facility (asset) related incidents. The system shall collect the following type of incident information for access by IMARS user query and for exporting to FMSS: Date/Time; FMSS location; Name of person reporting incident information; Short description of incident; Long description of incident; Case incident #; Priority level; and Type of incident
	Automated National Catalog System (ANCS+)	The system shall interface with the Automated National Catalog System (ANCS+) for the purpose of accessing museum catalog information, including: Classification lines; Cultural Identity; Artist Maker; Eminent figure; Current value; Dates; Basis; and Catalog number
	Safety Management Information System (SMIS)	The system shall interface to SMIS in a TBD format. Candidate information for inclusion would include injury information relating to fire fighter injuries and information indicating the stage of the fire. IMARS should interact directly with SMIS when the incident involves injuries, illnesses, or property damage. It is important that the two systems share data to eliminate duplicate data entry. The requirements for reporting injuries and illnesses that occur to people on Department of the Interior premises are spelled out in 485 DM Chapter 7 ( <a href="http://elips.doi.gov">http://elips.doi.gov</a> )
	SMIS (email) Interface	When a first responder is entering a report for an incident involving an injury or illness to an employee or other type of individual other than a member of "the public," IMARS should automatically notify that person's supervisor via e-mail that the incident has occurred and that an accident report should be recorded in SMIS
	Resource Activity Management System (RAMS)	RAMS is a web-enabled management reporting and tracking tool for the Offices of Cultural Resources and Natural Resources.
	Listing of Outlaw Treachery (LOOT) system	IMARS shall provide the capability to access LOOT system. The following capabilities shall be available relative to LOOT information: provide an IMARS incident identifier number to LOOT; transfer information relevant to a specific IMARS incident identifier number (in a tbd format) to LOOT (and supplemental form); and receive information relevant to a specific IMARS incident identifier number (in a tbd format) from LOOT (and supplemental form)

<sup>4</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.

IMARS Module	System Interface	Nature of Interface <sup>4</sup>
	National Fire Plan Operations & Reporting System (NFPORS)	The system shall interface to NFPORS in a TBD format. Candidate information for accessing from NFPORS are fuels treatment projects such as prescribed burns and mechanical fuel thinning projects and information needed to populate the appropriate fields in the Fire Report.
	Wildland Fire Program Analysis (WFOA)	IMARS shall interface to the WFOA program in a TBD format for information extraction into WFOA. Candidate information for accessing from WFOA is TBD.
	List of Classified Structures (LCS) and the Cultural Landscapes Inventory (CLI) Systems.	When an incident is recorded in IMARS if a historic structure or a cultural landscape is involved, then some key identifier for the structure or the landscape should be entered as part of the IMARS data. Second, IMARS, LCS, and CLI must recognize each other, accept inquiries on-line, and present mutually agreed upon views of data of importance or interest to the requesting party.
	NPS Safety Management System (SMS) for roads	The system shall provide the capability to interface to the future NPS SMS for roads. SMS requirements are TBD. The system shall not prohibit having a future interface for transmitting incidents that qualify as transportation safety accidents to the future SMS. The types of accidents include: Alternate Transportation Accidents; Motor Carrier Accidents (for tour buses); Private Vehicle Accidents; and Rail and Water Accidents
	Federal Payroll and Personnel System (FPPS)	The system shall provide the capability to interface with FPPS. The system shall provide the capability to transmit incident information collected in the previous requirement to FPPS in a TBD format.
	Project Management Information System (PMIS)	PMIS interface details are TBD. NPS plans called for interfaces between PMIS and RAMS.
	Service wide Traffic Accident Reporting System (STARS)	The STARS system contains traffic accident data dating back to 1995. The Case Incident Reporting System (CIRS) has been for many parks the administrative mechanism for collecting the data for STARS. Other parks use alternative automated traffic accident collection systems or depend on hard copy reports. STARS interface details are TBD.
	Cellular Digital Packed Data (CDPD)	As part of IMARS Search and Rescue function support, support for the CDPD standard is required. CDPD is standard for data transmission over wireless cellular telephone networks. <a href="http://www.wirelessdata.org/develop/cdpdspec">www.wirelessdata.org/develop/cdpdspec</a>
	USGS Interagency Operational Picture (IOP)	IMARS shall provide the capability to interface with the USGS IOP an Internet Map Server (IMS) service. Services of interest include: fire, oil spills, and natural hazards. The data from these services could provide context and national information about what is going on that might impact parks.

#### 4.4.2 FWS / NWRS Specific IMARS Interface Requirements

The FWS will have one IMARS system with two distinct modules: the LEMIS (IMARS/FWS/OLE) system for FWS Office of Law Enforcement personnel and a separate module for National Wildlife Refuge System (NWRS) personnel. FWS special agents, wildlife inspectors, management, and administrative staff will continue to employ LEMIS as their primary Graphical User Interface. All existing data entry will continue in LEMIS with the use of common data warehousing techniques to exchange information between FWS and IMARS servers. NWRS personnel, however, will migrate to IMARS. The conceptual system architecture is shown in Figure 4-5 below.

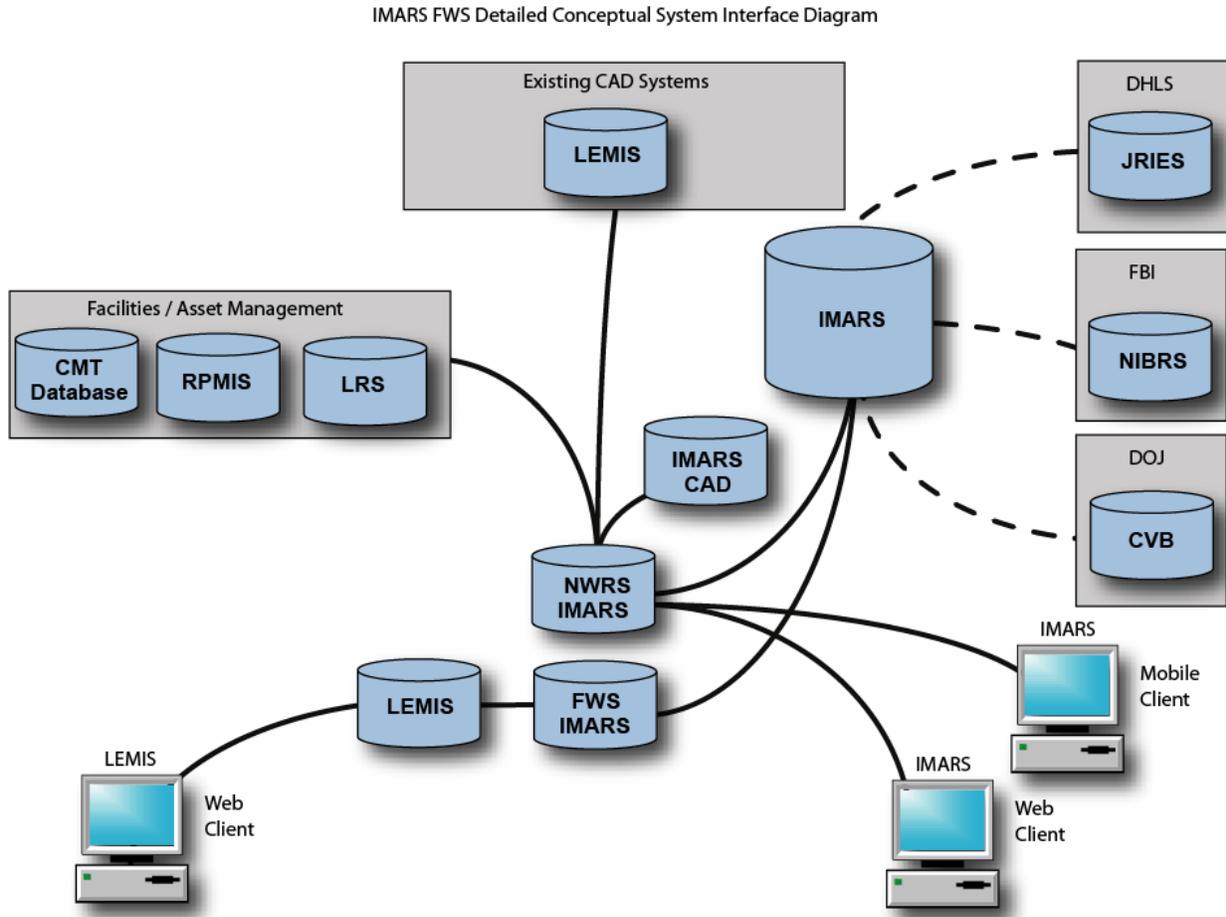


Figure 4-5. IMARS FWS / NWRS Detailed System Interface Diagram

Table 4-10 details the interface requirements between the FWS LEMIS server, the NWRS IMARS server, and Bureau, Departmental and external interfaces. The FWS has recommend the use of W3C Simple Object Access Protocol (SOAP) or American National Standards Institute X12 Electronic Data Exchange (ANSI X12 EDI) to implement information exchange between the LEMIS and IMARS servers. It is recommended that the exact nature of the interface, the information exchange mechanism, and the frequency of updates / information exchanges be thoroughly documented during the FWS and NWRS pilots.

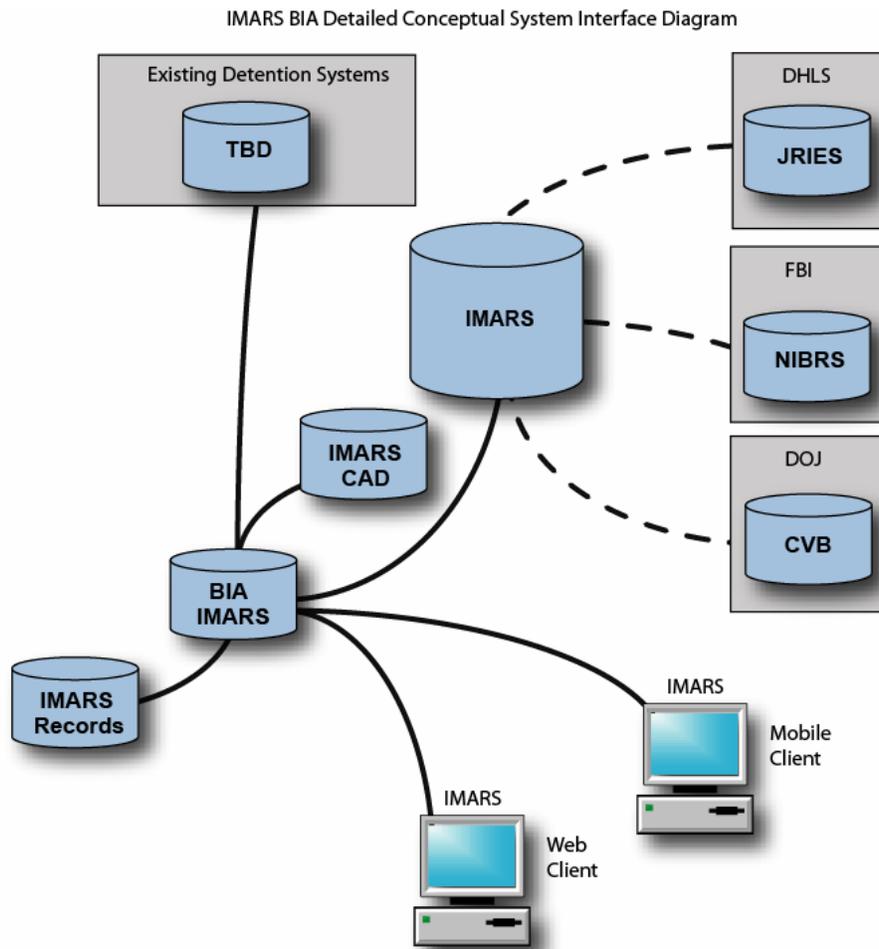
**Table 4-10. IMARS FWS / NWRS System Interfaces**

IMARS Module	System Interface	Nature of Interface <sup>5</sup>
IMARS FWS	LEMIS	FWS special agents, wildlife inspectors, management, and administrative staff will continue to employ LEMIS as their primary Graphical User Interface. All existing data entry will continue in LEMIS with the use of common data warehousing techniques to exchange information between FWS and IMARS servers. Per DOI standards, use of W3C Simple Object Access Protocol ( W3C SOAP) or American National Standards Institute X12 Electronic Data Exchange (ANSI X12 EDI) are preferred to achieve data exchange between IMARS and the FWS module.
IMARS NWRS	FWS CMT Database	The FWS CMT database maintains all “official” Refuge information such as physical and mailing addresses. IMARS/FWS//RLE will use this information as the source of refuge-related data information as the source of refuge-related data.
	FBI’s National Crime Information Center (NCIC) System	NCIC/DOJ - IMARS/FWS/RLE should provide the ability to send and retrieve information from this database.
	Real Property Management Information System (RPMIS)	IMARS NWRS shall interface with RPMIS which tracks and manages real property on Service Refuges.
	Land Records System (LRS)	IMARS NWRS shall interface with LRS which tracks parcels owned and/or leased by FWS and included in the Refuge System

### 4.4.3 BIA Specific IMARS Interface Requirements

The BIA differs in that it has significant requirements for support of its current and planned detention center systems. The interfaces to these existing and planned detention systems are not well defined nor are the systems themselves discussed in any detail. These conceptual system interfaces are shown in Figure 4-6 below.

<sup>5</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.



**Figure 4-6. IMARS BIA Detailed System Interface Diagram**

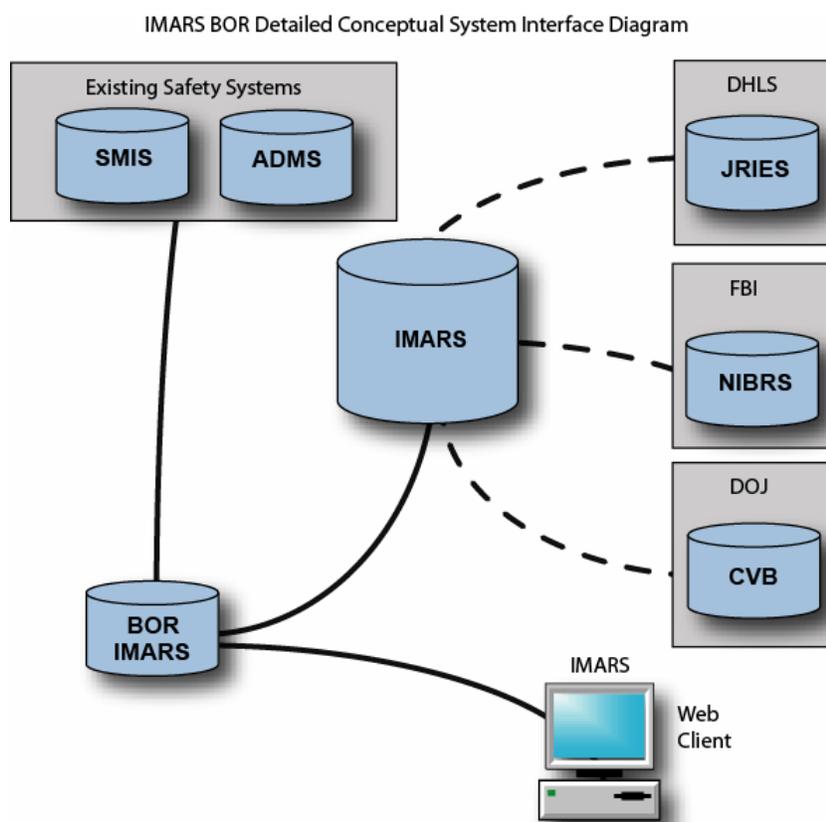
The following table details the interface requirements between the BIA IMARS server and potential detention center systems (planned and existing). The exact nature of these interfaces and detention center systems is not defined. Having such vague system interface requirements may introduce implementation / schedule risk to the BIA IMARS implementation unless adequately addressed. It is recommended that during the implementation BIA IMARS pilot, the exact nature of the interface, the information exchange mechanism, and the frequency of updates / information exchanges be thoroughly documented. It is also recommended that existing and planned BIA detention center systems be thoroughly documented. In cases where information exchanges will occur between the BIA IMARS implementation and these systems, data models of these existing detention center systems should be acquired. Finally, it is recommended that the BIA use W3C Simple Object Access Protocol (SOAP) or American National Standards Institute X12 Electronic Data Exchange (ANSI X12 EDI) to implement information exchanges between existing/planned BIA systems and IMARS.

**Table 4-9 IMARS BIA System Interfaces**

IMARS Module	System Interface	Nature of Interface <sup>6</sup>
IMARS BIA	FBI's National Crime Information Center (NCIC) System	IMARS must interface with the NCIC system ( <a href="http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm">http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm</a> ). The system must be able to add and pull information from States that require a Child Abuse Registry.
	Detention Center Systems	The BIA has multiple requirements for interfacing to existing and planned Detention Center Systems. IMARS should support the capability for telephone systems to be linked to an IMARS automated call tracking system. IMARS should also interface with the Records Management System (RMS) and the Computer Aided Dispatch (CAD) via a central data repository

#### 4.4.4 BOR Specific IMARS Interface Requirements

The BOR has some limited interface requires to existing facilities safety management systems. The BOR is currently working with the FWS to track law enforcement and security incidents within LEMIS. The BOR requires that all collected incidents within LEMIS must be migrated to the new IMARS system. These conceptual system interfaces are shown in Figure 4-7.



**Figure 4-7. IMARS BOR Detailed System Interface Diagram**

<sup>6</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.

The following table details the interface requirements between the BOR IMARS server and its Bureau, Departmental, and external interfaces. The BOR also has requirements for the one-time migration of its current incident data (stored in a BOR-implementation of LEMIS) to IMARS. The IMARS Functional Requirements document had very limited information on the exact nature of the interfaces to these existing systems, but the lack of details on the IMARS data model and the lack of a detailed IMARS information exchange plan was cited by the BOR as the reason for this lack of detail. The BOR may also have BOR-specific requirements for its interface to the DHLS’s JRIES system and a need to support a currently non-automated Emergency Notification System which provides prompt and direct communication of serious incidents occurring at Reclamation facilities to the Commissioner and the DOI Watch Office. It is recommended that the exact nature of the interface, the information exchange mechanism, and the frequency of updates / information exchanges be thoroughly documented during the BOR pilot

**Table 4-10 IMARS BOR System Interfaces**

IMARS Module	System Interface	Nature of Interface <sup>7</sup>
IMARS BOR	Safety Management Information System (SMIS)	IMARS must integrate / interface with the Department of Interior's SMIS in order to capture the Safety and Occupational Health Reporting requirements established by DOI directive
	ADMS	Life Safety Code (LSC) compliance issues may be substantial in facility based incidents with subsequent injury to inhabitants; the IMARS must be capable of integrating the current database system (ADMS) used to track LSC compliance status.

#### **4.4.5 BLM Specific IMARS Interface Requirements**

The BLM has no Bureau – specific interface requirements. The conceptual system interfaces are shown in Figure 4-8.

<sup>7</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.

IMARS BLM Detailed Conceptual System Interface Diagram

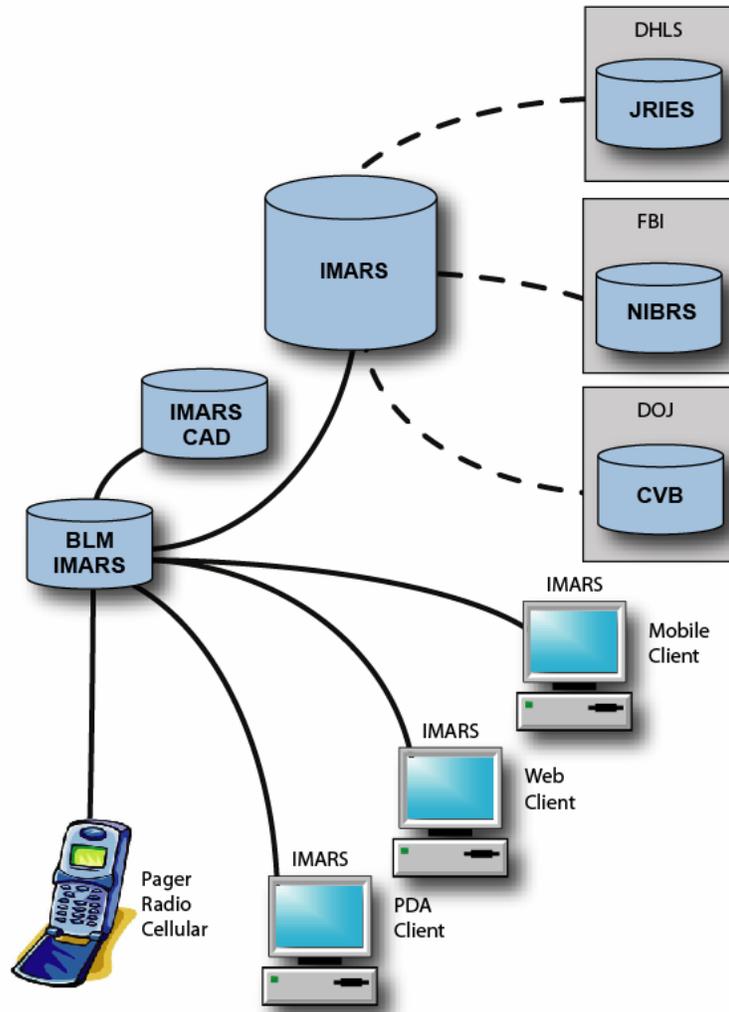


Figure 4-8. IMARS BLM Detailed System Interface Diagram

The BLM has no Bureau – specific interface requirements. The nature of its interfaces to CVB and NIBRS is shown in Table 4-11 below.

Table 4-11. IMARS BLM System Interfaces

IMARS Module	System Interface	Nature of Interface <sup>8</sup>
IMARS BLM	Central Violations Bureau (CVB).	According to the BLM, there are no BLM specific interface requirements that are not addressed by the DOI IMARS requirements. The LAWNET 2.0 SRS document does specify a CVB external interface requirement which is addressed by the central DOI IMARS server to CVB interface.
	FBI National Incident-Based Reporting System (NIBRS).	The LAWNET 2.0 SRS document does specify a NIBRS interface which is addressed by the central DOI IMARS server to NIBRS interface.

<sup>8</sup> Note: The system interfaces and the nature of these interfaces were taken directly from available IMARS Functional Requirements documents.

## 4.5 Technology Findings & Recommendations

Technology findings refer to the findings where the LOB is dealing with non-standardized or obsolete technologies or architectures.

**Technology Finding 1** - *Current Law Enforcement Systems are not integrated and have deployed non-shared, Bureau-specific infrastructure investments.*

Figure 4-9 shows the current DOI Law Enforcement system architecture. The figure shows multiple, stand alone systems with no systems automating law enforcement functions at the BIA and BOR. Currently there is no direct external connection for annual upwards reporting from LAWNET to NIBRS, the FBI uniform incident data collection system. LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report; however LAWNET does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, report crime statistics to the DOJ/FBI through the Department. Since the Department of Interior has yet to switch to NIBRS from UCR format of reporting, the BLM is reporting crime statistics in the UCR format even though it is NIBRS compliant. The UCR is submitted once a year around March and includes crime statistics for the previous calendar year. NPS CRIMES and CIRS incident data is specific to a given park, the LEMIS NWRS module (LEMIS Incidents) and LEMIS data are specific to the FWS, and LAWNET data is specific to the BLM. System architectures vary from the FWS's J2EE web client applications (LEMIS and LEMIS Incidents) to DOS-based systems with proprietary Clipper databases for the NPS and BLM.

Figure 4-9 shows that data common to both FWS NWRS (LE-IMAGS) and FWS OLE (LEMIS) will occur only once in a shared data repository. It should be noted that NWRS-specific data will reside in its own database and OLE-specific data will reside in its own database.

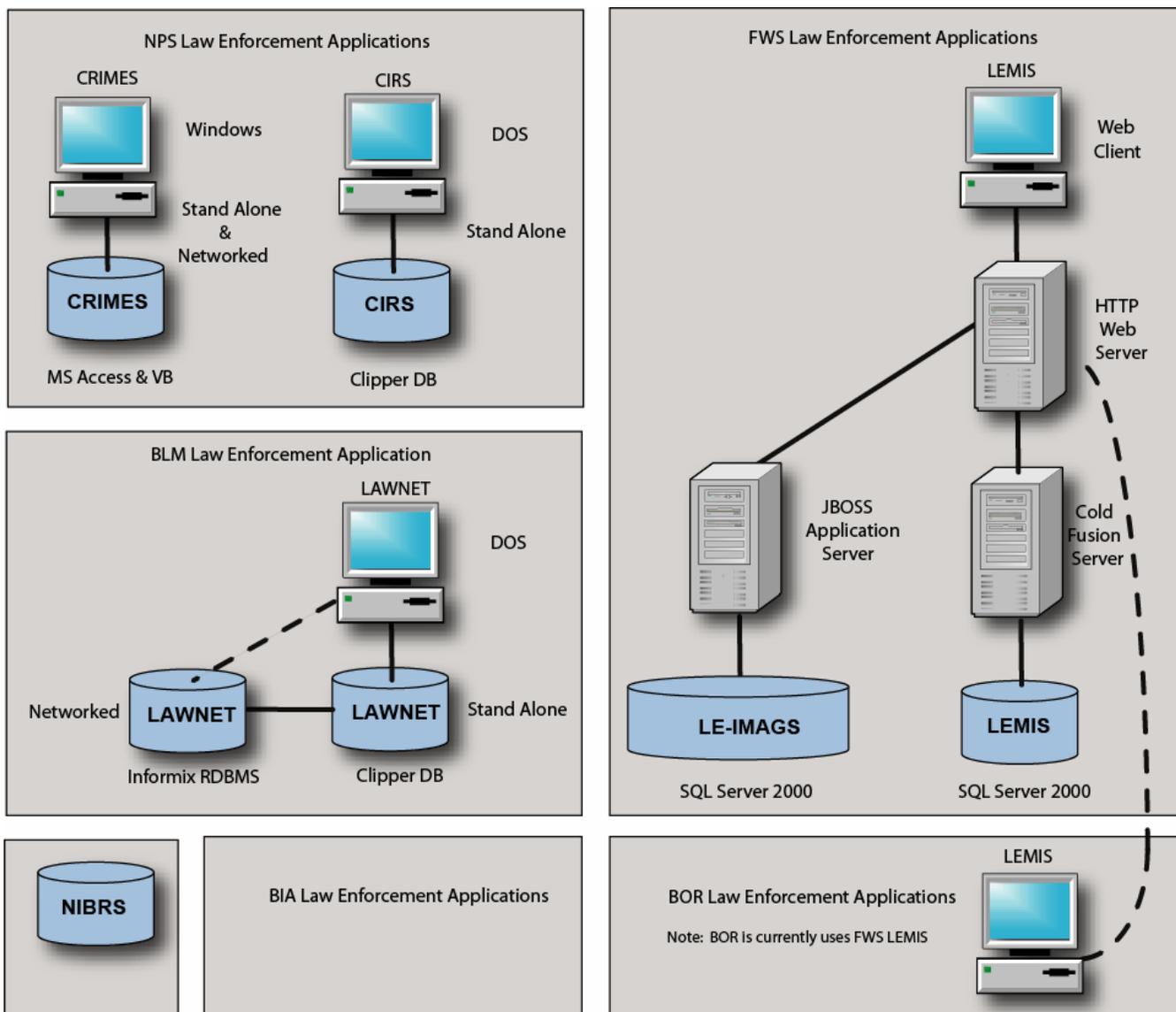


Figure 4-9. Law Enforcement “As Is” Conceptual System Architecture

The short comings of the current, non-integrated Law Enforcement Systems are addressed by the Department-wide IMARS procurement. LAWNET, CIRS, CRIMES, and non-core LEMIS modules will be retired and replaced by IMARS. Non-core LEMIS requirements (i.e. LEMIS Declarations, case law, etc.) will initially remain in the LEMIS system and be evaluated for inclusion as IMARS evolves.

**Technology Finding 2** - Only two systems, LEMIS and LE-IMAGS use Active-Directory user authentication. All other law enforcement systems have individual means of tracking user authentication.

It is recommended that current DOI law enforcement applications migrate to the use of Active Directory as their authentication mechanism. It is also recommended that any new law enforcement procurement (e.g. IMARS) implement Active Directory as its user authentication mechanism. Most current DOI law enforcement applications maintain their own user list and passwords.

**Technology Finding 3** - BLM’s LAWNET and NPS’s CIRS systems are based on end-of-life DOS technology.

Both LAWNET and CIRS use DOS-based Clipper databases and user interfaces. The IMARS procurement will address the need to replace this outdated technology. Fortunately, the LAWNET application has a centralized Informix RDBMS in addition to the Clipper DOS clients. Thus migration of LAWNET data to any proposed IMARS system will be feasible.

**Technology Finding 4** - *NPS's CRIMES is based on MS Access database technology that has reached the 1GB database size limit of MS Access for certain larger National Parks.*

NPS operates two law enforcement applications: the CRIMES incident data collection application and the retired CIRS application. CIRS is a DOS-based Clipper application whereas CRIMES is a home grown MS Access database application. Neither application is centralized or web-enabled. MS Access has a 1GB database size limitation that is being exceeded as some larger national parks.

As an interim solution, the DOI may wish to investigate the web-enablement of the CRIMES application and the migration of all current CIRS users to the new web-enabled CRIMES application. This would be an interim solution under the guise of data migration prior to deployment of IMARS. This interim solution would likely use a .NET architecture and a SQL Server RDBMS. The solution could also implement Active Directory as its authentication mechanism.

**Technology Finding 5** - *The LEMIS and LE IMAGS systems are J2EE-compliant systems. In all instances where LEMIS and LE IMAGS modules have common business functions, only one instance of code is used and only one database component is used. As of 12/31/2004 LEMIS and LE IMAGS will share the same authentication mechanism – Active Directory.*

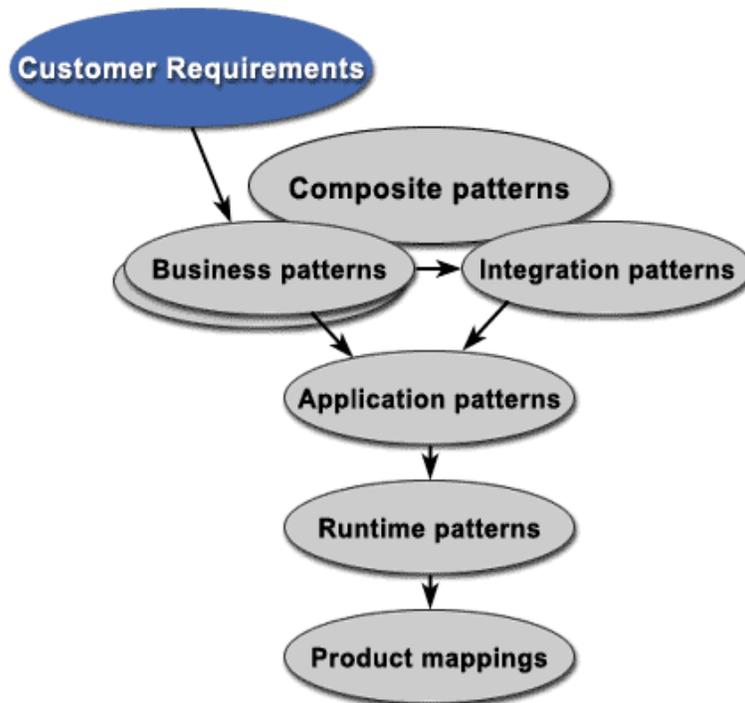
It is recommended that LEMIS and LE IMAGS functional modules that are redundant to IMARS be replaced by IMARS after FWS acceptance testing and successful data migration. It is also recommended that FWS-specific asset management databases under the LEMIS module be examined for possible migration to enterprise asset management solutions such as MAXIMO

**Technology Finding 6** – *There are differences between IMARS Functional Requirements and Bureau-specific TRM implementations.*

The IMARS Functional Requirements document specifies the server operating system software as Microsoft Windows 2003 and the relational database management system (RDBMS) software as Oracle 9.2.0.4 or higher. In some cases, Bureau-specific standards for RDBMS software and server operating systems differ from the set IMARS requirement. The BLM, for example, standardized on Informix for its RDBMS implementation and the FWS appears to be implementing enterprise systems on SQL Server 2003. Unless TRM standards for RDBMS are standardized across all Bureaus, IMARS will likely need to be implemented as RDBMS neutral. It is not uncommon for vendors to create solutions that are specific tied to a single vendor – notably Oracle 9iAS technology. This finding does not imply that Bureaus have the option of non-compliance with the DOI TRM. It does highlight the heterogeneous nature of the DOI's technical environment.

**Technology Finding 7** - *IMARS will address the system-specific infrastructures of the current environment by featuring reusable technical components in a standards-based solution architecture using patterns.*

Successful transition from Enterprise to Solution Architecture is one of the most important steps in deriving value from an Enterprise Architecture effort. Patterns can play an important role in solution level architecture by identifying appropriate system building blocks and topologies. When aligned with an organization's Enterprise Architecture, patterns become a powerful tool for developing EA compliant Solution Architecture. Figure 4-10 shows a diagram of the relationship of patterns to the solution development process.



**Figure 4-10. Diagram Showing Relationship of Patterns to Solution Development Process**

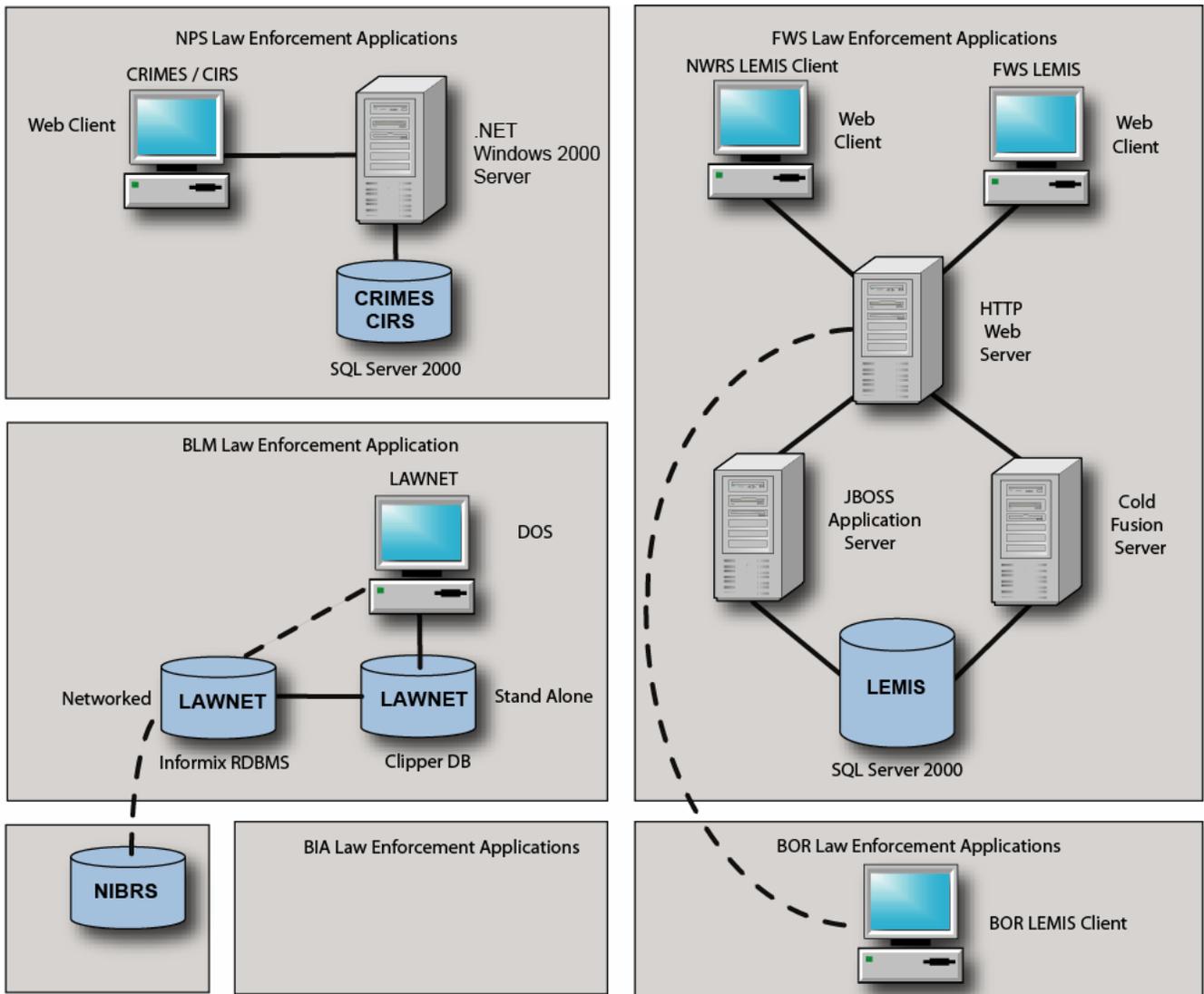
As the architecture of IMARS is considered in progressively greater detail, patterns will provide a straightforward way to highlight architecturally significant requirements and identify appropriate architectural approaches and topologies. These patterns can be aligned with DOI's tactical and strategic architectural principles and guidelines that are captured in artifacts such as the DEAR and DOI's FEA based reference models, e-Government Interoperability Model, Service Oriented Application Model. That alignment creates a framework for architecting an IMARS solution that is harmonized with DOI's EA principles and guidelines.

Patterns also play a significant role in the incorporation of uniform security features across an enterprise. The DOI is currently assessing the adoption of a security architecture that leverages patterns. This pattern-driven approach provides a consistent, comprehensive approach to defining security architecture at both enterprise-wide and individual solution levels.

## **5. Transition Plan**

### **5.1 Tactical Recommendations:**

Any tactical recommendations must be viewed in the context of the planned IMARS procurement. The FWS and NWRS have a working declarations and incident management system (LEMIS / LEMIS NWRS module). BOR is currently leveraging the LEMIS application and have stated upon the deployment of IMARS, they will need to migrate their existing LEMIS incident data into IMARS. The timely deployment of IMARS for the BLM, BIA, and NPS should take top priority for the DOI. The complete adoption of IMARS, however, may take years thus the DOI should consider possible interim solutions. Figure 5-1 shows the proposed interim system architecture for the Law Enforcement LOB. The NPS Law Enforcement applications have been re-designed to leverage common infrastructure components and a common authentication model and data have been migrated from multiple CIRS and CRIMES stand alone databases to a consolidated SQL Server database. A simple .NET architecture is used to take the existing Visual Basic application and MS Access database and to migrate the data to a SQL Server 2000 database with a Web-client. This has the added advantage of providing a single database to migrate to the proposed future IMARS system and migrating users off end-of-life DOS Clipper clients. The effort forces consolidation of the CIRS and CRIMES data stores into a single RDBMS. This will require modeling of the CRIMES and CIRS databases and migration of a significant amount of data but will simplify data migration to IMARS. This interim solution for the NPS should be viewed as prudent risk mitigation (in the event that IMARS is delayed) and as a step in data consolidation, review, and migration to IMARS.



**Figure 5-1. Law Enforcement “Interim” Conceptual System Architecture**

The FWS LEMIS module will be re-engineered to leverage existing ADS infrastructure for authentication/authorization. This infrastructure is now in place for the RLE module (LE-IMAGS). LEMIS and LE-IMAGS will share a common database schema where appropriate, and will implement a conceptual interface architecture similar to Figure 4-3 (on page 26) for data specific to each application. The current LE-IMAGS application uses a simplistic GIS data capture mechanism whereby users navigate a map and click on the map to input the location of an incident. This limited GIS functionality may be incorporated into LEMIS as part of this interim solution. This interim solution assumes the IMARS procurement would take upwards of 12 months and that data migration of CIRS and CRIMES data to the IMARS system is a requirement / desirable. Given the limited number of BLM law enforcement personnel and the relative functional adequacy of the BLM LAWNET system, no changes have been made to LAWNET for this interim solution.

## 5.2 Strategic Recommendations

The “To-Be” architecture for the Law Enforcement LOB will be largely a function of the IMARS procurement. Whether the architecture is J2EE or .Net remains to be seen. We can, however, portray near term and long term strategic architectures that are technology neutral. Figure 5-2 shows the near-term “To-Be” Conceptual System Architecture for the Law Enforcement LOB. The FWS LE-IMAGS and LEMIS applications now share the IMARS database. The BLM, BOR, BIA, and NPS all have standardized on IMARS. FWS asset management applications (e.g. eagle parts, seized assets, etc.) have been migrated to MAXIMO. At this stage, LE-IMAGS should be seriously considered for retirement as its functionality is redundant to IMARS. The use of the IMARS database allows the FWS to be NIBRS-compliant.

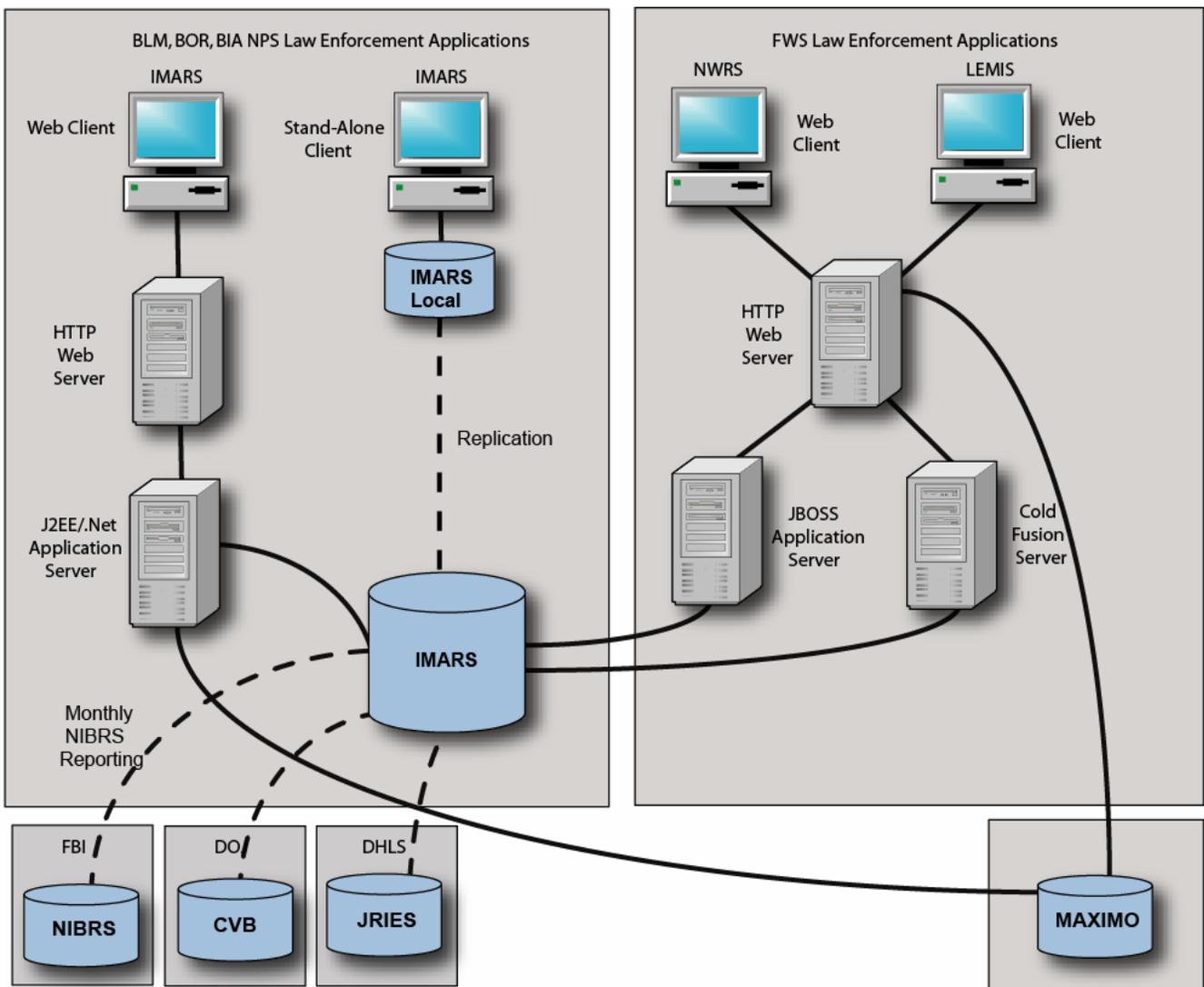


Figure 5-2. Law Enforcement Near-Term “To-Be” Conceptual System Architecture

Figure 5-3 shows the long-term “To-Be” Conceptual System Architecture for the Law Enforcement LOB. The vision for the long-term architecture calls for law enforcement LOB to leverage the proposed IMARS system architecture across the DOI. LEMIS application servers are retired along with their associated dedicated development staff and support infrastructure. The FWS LEMIS application is now

a declarations module under IMARS. In order to be successful the proposed IMARS application must meet the diverse law enforcement needs of all bureaus.

The proposed IMARS system also leverages a number of DOI-wide and government-wide services such as Pay.Gov (payment collection for the IMARS declarations module); FBMS (time and reporting); and Geospatial One-Stop (map visualization services). The vision of this future IMARS system would be leverage existing web services where feasible. The IMARS system would interface with legacy and existing data repositories using an enterprise integration bus, an integration server, and a series of adaptors.

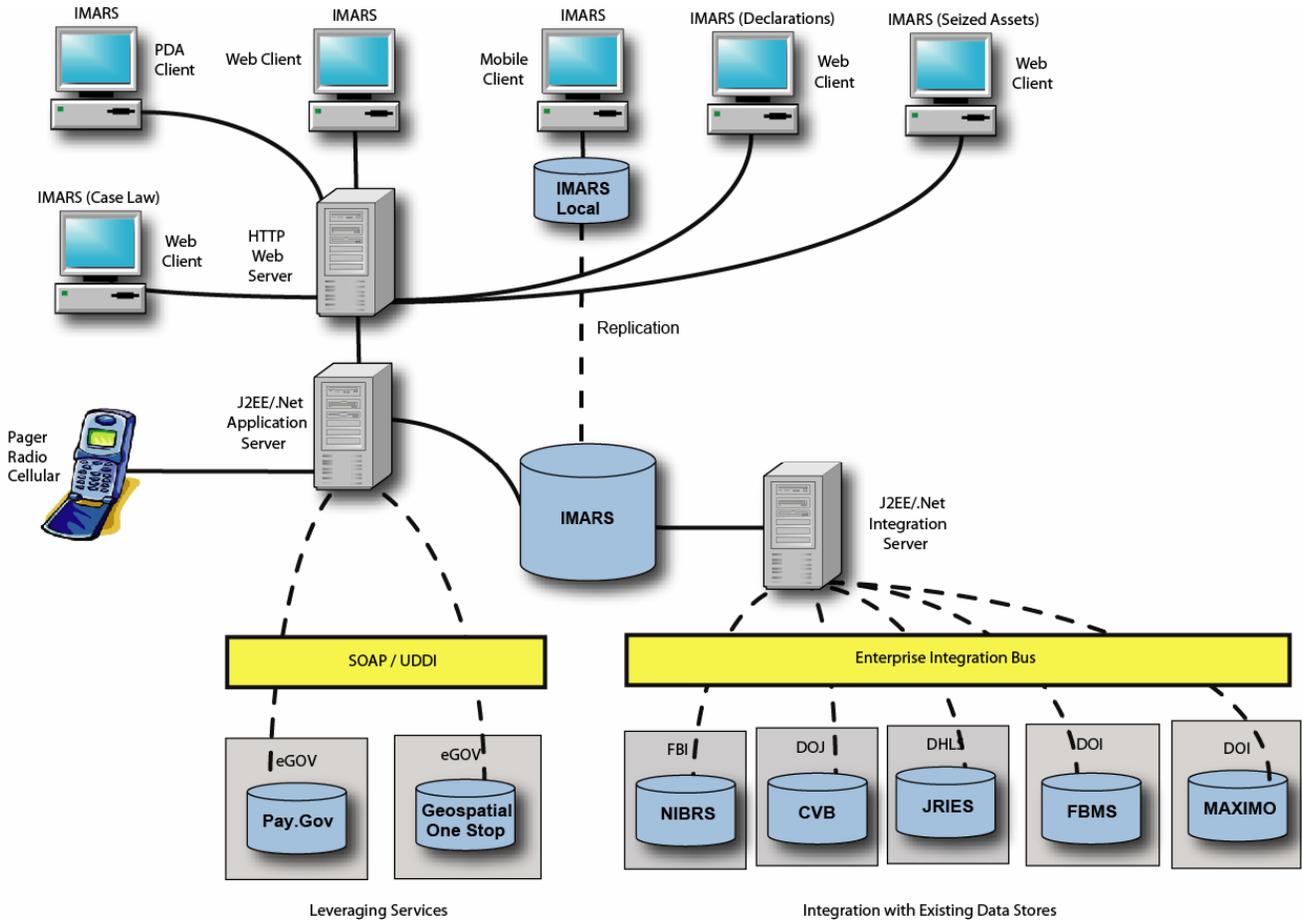


Figure 5-3. Law Enforcement Long-Term “To-Be” Conceptual System Architecture

## 6. References

Through a collaborative Interior-wide process, the IEA Common Requirements Vision (CRV) was developed and published on October 15, 2001. This vision document is intended to ensure that Interior's IT products and services are aligned with the business community's strategic direction. Subsequently, the IEA Conceptual Architecture Principles (CAP) was published in January 2002. The CAP identifies a logically consistent set of principles derived from the business requirements in the CRV. These principles guide the engineering of the organization's information systems and technology infrastructure. The approach, methodology and supporting criteria for developing Interior's modernization blueprint is based on the above documents, which may be reviewed at: <http://www.doi.gov/ocio/architecture/>.

- *Business Reference Model (BRM) Version 2.0 Release Document* - This document outlines the definition of the Business Reference Model Version 2.0. It includes the BRM creation and validation processes, as well as detailed descriptions of the Federal Business Areas, Lines of Business, Sub-Functions and Modes of Delivery.
- *Performance Reference Model (PRM) Version 1.0 Release Document Volume I* - This document describes the PRM and provides information about why a PRM is needed, who can benefit from using it, and how the PRM was developed.
- *Performance Reference Model (PRM) Version 1.0 Release Document Volume II* - This document discusses how the PRM can be used through the IT life cycle and identifies integration points with other key management processes, including agency IT CPIC, EA, GPRA, PART, and the budget process.
- *Service Component Reference Model (SRM) Version 1.0 Release Document* - This document outlines the definition of the Service Component Reference Model Version 1.0. It includes the SRM creation and validation processes, as well as detailed descriptions of the Federal Service Domains, Types and Components.
- *Technical Reference Model (TRM) Version 1.1 Release Document* - This document outlines the definition of the Technical Reference Model Version 1.1. It includes the TRM creation and validation processes, as well as detailed descriptions of the Federal Service Areas, Categories, Standards and Specifications.
- *FEA Federal Reference Models (BRM, SRM, TRM) Version 1.2: XML Document* - This document is the part of the Federal Enterprise Architecture relating to the BRM v2.0, SRM v1.0, and the TRM v1.1. It includes the various layers of the Federal Reference Models and their detailed descriptions.
- *E-Gov Enterprise Architecture Guidance (Common Reference Model)* - This document describes a federal e-government target conceptual architecture. The architecture is based on the business requirements derived from the initiatives as well as system engineering design best practices. It provides a workable description of the components needed by e-government initiatives and business activities to move rapidly into the web service-enabled business transaction environment.
- *FEA A-11 Additional Guidance Document* - This document provides detailed guidance and examples to help agencies complete the FEA-related requirements, and to help them complete questions in the OMB Exhibits 53 and 300 for IT investments. This document is intended for IT project managers or senior analysts completing these exhibits for submission to OMB.

To define the Law Enforcement As-Is Business Architecture, data was gathered across organizational boundaries. Interviews were conducted with BLM, NPS, FWS, and BOR personnel. Existing Law Enforcement application architecture artifacts were reviewed, placed into the context of the OMB

Federal Enterprise Architecture (FEA) Reference Models, and where appropriate imported into the DOI Enterprise Architecture Repository (DEAR) modeling tool. In addition to the above general references, the following documents were examined in support of this report:

- *U.S. Department of the Interior Technical Assistance for Information Technology Investment Management CIO Score Card and Checklist for IMARS*, May 23, 2003 – This DOI-OCIO capital planning document provided a scoring of the IMARS business case with identified gaps and/or weak points of the business case.
- *LE IMAGS OMB Exhibit 300-1 Project Profile*, FY 2004 – This OMB submission document provided a high-level overview of the LE IMAGS application.
- *LEMIS/IMARS Exhibit 300-1 Project Profile*, FY 2004 – This OMB submission document provided a high-level overview of the LEMIS/IMARS application
- Misc. LEMIS 2000 Training Material – LEMIS 2000 training material was used to augment hands-on use of the LEMIS application and interviews with LEMIS users and developers.
- Misc. LAWNET Training Material – LAWNET training material was used to augment interviews with LAWNET users and developers.
- *LAWNET Exhibit 300-1 Project Profile*, FY 2004 – This OMB submission document provided a high-level overview of the LAWNET application
- *IMARS Exhibit 300*, January, 20, 2004 – This OMB business case submission document (DRAFT) provided a more detailed view of the proposed IMARS application.
- *Law Enforcement Data Modeling Report on Initial Modeling Work*, March 2004 – This documented, created by IT Pioneers, provided some high-level enterprise data architecture input for the Law Enforcement LoB.
- *National Park Service Incident Reporting and Data Management System Needs Assessment and Recommendations*, September 10, 2002 – This detailed requirements document created by TRW provided background input for Law Enforcement LoB business requirements.

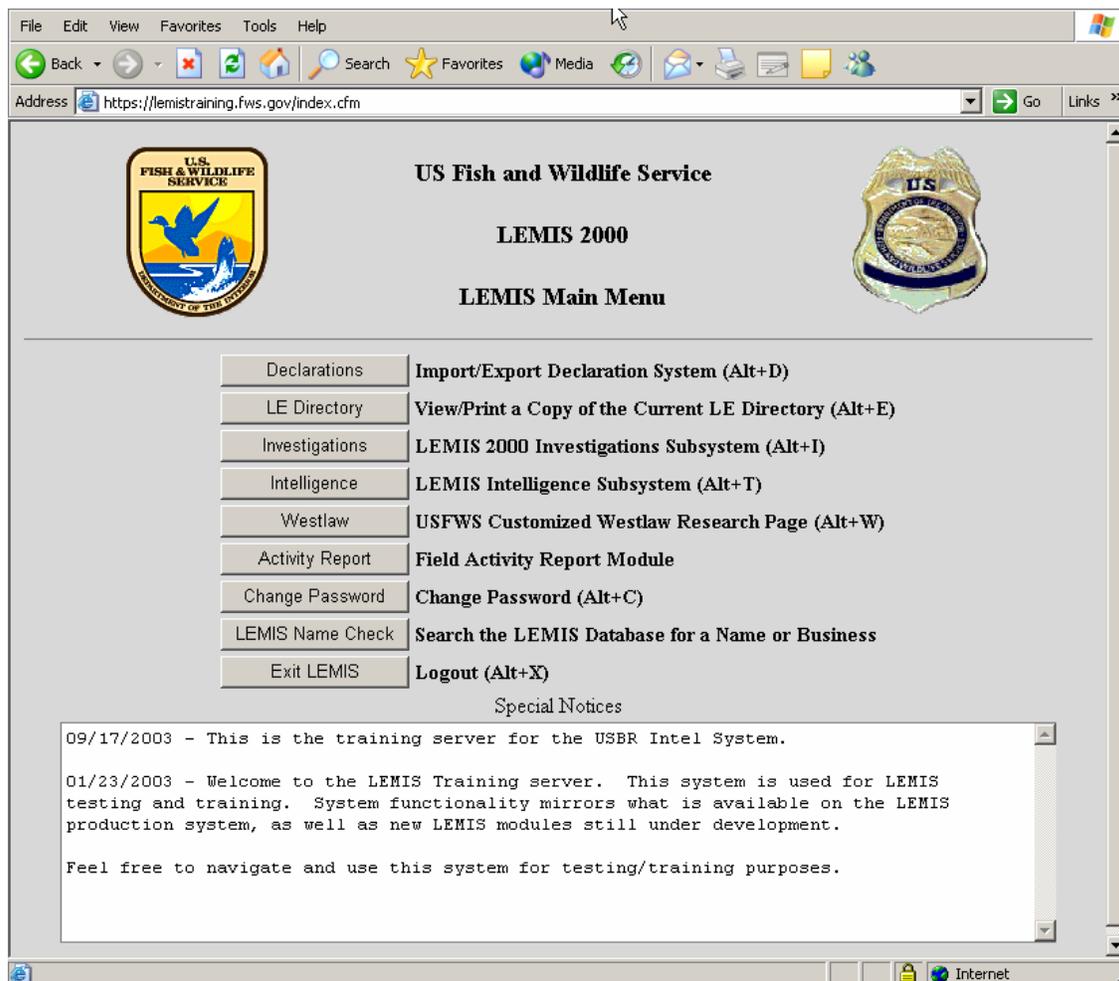
**Appendix A - Supporting Analytical reports derived from the DOI Enterprise Architecture Repository (DEAR)**

## Appendix B - Supporting Analytical reports derived from interviews with Law Enforcement LOB system owners, developers, and users

### B-1. LEMIS 2000 Application

#### *General Information on LEMIS 2000*

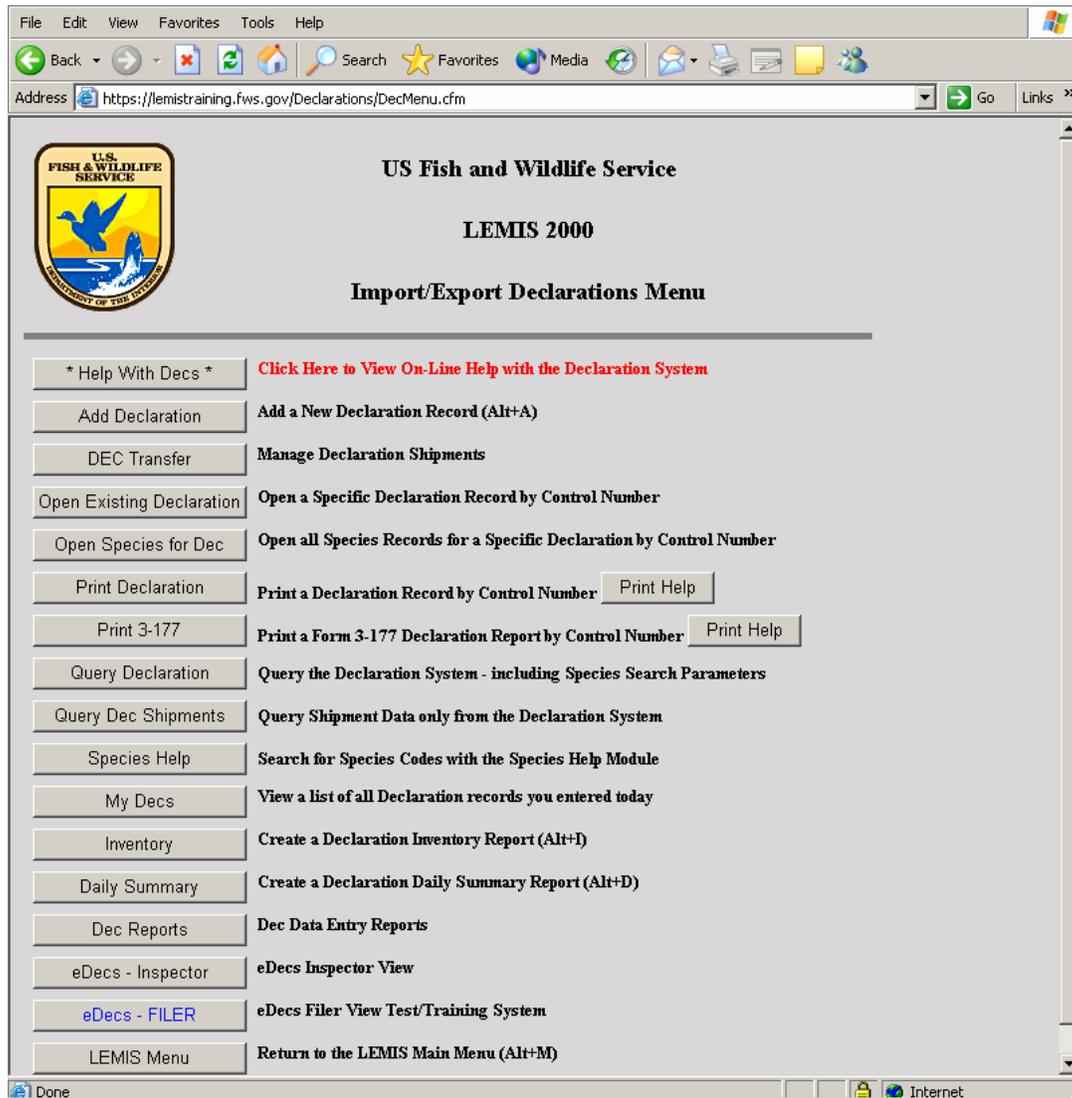
LEMIS 2000 is a Cold Fusion MX and SQL Server 2000 Application. The application is a server-based web application. It requires a dedicated internet (TCP/IP) connection to the central server. No disconnected mode is available. There are a total of four LEMIS 2000 servers: a secure production server, a training server (also inside the firewall), a development server, and a non-secure (outside the firewall) eDEC module server. There are no failover servers, but all LEMIS 2000 servers essentially the same and thus the training server could be quickly reconfigured to take over should a failure occur on the production server. It's not entirely clear how back-up and recovery takes place with respect to the LEMIS 2000 servers. LEMIS system development uses Macromedia's JRUN which allows LEMIS developers to create hybrid applications that combine ColdFusion pages with back-end logic written in Java.



*LEMIS 2000 Main Screen*

There are currently 600 users of the LEMIS 2000 system and its modules. LEMIS uses its own access control and authentication mechanism. LEMIS does not use Active Directory, but future integration of LEMIS 2000 to incorporate Active Directory is planned. LEMIS has various modules that are all Web-

based forms and reports. Modules include import/export declarations, investigations, intelligence (queries), field activity reports (incident reports), and case law research. The import / export declarations sub-menu is extensive with an impressive array of FWS-specific forms and reports.



***LEMIS 2000 Import / Export Declarations Sub-Menu***

***Some observations concerning LEMIS 2000:***

1. There is no spell checker. The user acceptance of LEMIS 2000 is brought into question when it requires a full-time administrative assistant for every 3 to 8 law enforcement officers. There appears to be limited error checking built-into the LEMIS application.
2. The LID (FWS Criminal database module of LEMIS) has no fingerprints or connections with external criminal database systems such as NCIC or RMIN (Rocky Mountain Information Database). NCIC is a computerized index of criminal justice information (i.e.- criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies.
3. Seized property tracking is performed using a separate inventory system which appears to be an outdated Visual Basic application. A proposed add-on to LEMIS will track cadavers and parts of

endangered eagles. This module (National Eagle Repository Database) will track the collection and disposition of these eagle parts to Native Americans.

4. FWS forensic personnel original had a tie-in to LEMIS. A forensic module was created specifically for this user group, but the forensic personnel refused to use the module. As such, all forensic information is added in paper form to case files, but is not put into the LEMIS system. It would seem logical that this collected body of forensic information would be valuable for inspectors and agents to query.
5. There is a large body of additional documentation that is not included as part of the LEMIS electronic case file. These include pictures, documents, forensic reports, and other hardcopy data. Most records management systems allow for the scanning and attachment of these additional documents to the electronic case file. The official paper case files are kept in the local office for one year after they are closed and then moved to archival storage for up to 20 years.
6. Another planned add-on module is the Covert Financial Tracking system. This is largely an administrative module for tracking costs associated with certain covert investigative (e.g. “sting”) operations. Any financial tracking appears to have potential overlap with FBMS.
7. eDOCs is a very successful LEMIS module. eDOCS allows citizens to fill-in a Form 3-177 import / export declaration on-line. Citizens may also fill-in a Form 3-177 by downloading and printing a PDF file and then submitting this form manually. These hardcopy forms are then placed into eDOCS using a native American firm located in Bismarck, ND. There are also additional documents which are scanned. The company performing the Form 3-177 data has requested a QA module to better assist them in filling in these forms from the hardcopy originals. Also, the eDOCs module was originally designed to accept credit cards. It is being expanded to work with the Pay.Gov system and accept a wider form of payments
8. LEMIS has some very limited geospatial links. Within the LID, there’s a link to MapQuest to view personnel location information. The LEMIS application simply passes the address to MapQuest and a map is then displayed in a window.

### ***LEMIS 2000 User Groups***

In terms of user groups, there are Wildlife Inspectors (typically work at port locations), Special Agents, Legal / Administrative Assistants, and LEMIS System Administrators.

<b>FWS LEMIS User</b>	<b>User Role</b>	<b>Modules Used</b>
Special Agent	Conducts investigations, collects intelligence, assists in prosecution, manages cases, coordinates with other law enforcement agencies, conducts legal research for cases, conducts time and reporting on law enforcement activities	Declarations, Investigations, Intelligence, Westlaw, Search, and Activity Report
Wildlife Inspector	Works primarily with import / export declarations.	Declarations and Activity Report
Administrative / Legal Assistant	Assists Special Agents in the filling-in and management of case information. Typically there are administrative assistants assigned to every 3 to 8 Special Agents who’s primary function is to input, review, and QA case-related information.	Declarations, Investigations, Intelligence, Westlaw and Search

FWS LEMIS User	User Role	Modules Used
LEMIS Administrator	Has administrative access to LEMIS application. Adds, deletes, updates user information and access control.	Access Control

***LEMIS 2000 Business Functions Supported***

At the very highest level of abstraction, the FWS law enforcement line of business appears to perform three primary functions: investigations, enforcement, and inspections. Unlike the BIA, the FWS law enforcement line of business does not incarcerate individuals. Typically, when arrests are made, these are done in coordination with local law enforcement officials.

Investigations	<ol style="list-style-type: none"> <li>1. Open a new case</li> <li>2. Review a case</li> <li>3. Query cases</li> <li>4. Conduct legal research on a case</li> <li>5. Perform intelligence activities</li> </ol>
Enforcement	<ol style="list-style-type: none"> <li>1. Perform patrols</li> <li>2. Make arrests</li> <li>3. Process violations</li> <li>4. Collect fines</li> <li>5. Conduct Investigations</li> </ol>
Inspections	<ol style="list-style-type: none"> <li>1. Add declaration (Web-bases &amp; Hardcopy)</li> <li>2. Collect fees (associated with Shipments)</li> <li>3. Query declarations</li> <li>4. Inspect shipment</li> <li>5. Approve shipment</li> <li>6. Confiscate shipment</li> <li>7. Add confiscated item to inventory control</li> <li>8. Edit / update declaration</li> </ol>

***LEMIS 2000 External Law Enforcement Links***

Based on interviews with LEMIS 2000 users, it appears that FWS law enforcement personnel work closely with other State / Local law enforcement personnel. FWS violations are prosecuted in State and Federal courts. Adjudication (status) of the case is manually updated into LEMIS. LEMIS does not have electronic transfer of reports to other law enforcement agencies. LEMIS tracks who received documents, but these are printed and then mailed or Faxed to their recipients.

When performing port inspections, FWS personnel work closely with Customs and APHIS personnel. Customs is currently in the process of creating a single application for tracking international trade shipments (International Trade Data System or ITDS). There have been talks with FWS about being the managing partner for this proposed system. Apparently upwards of 30 million dollars has been earmarked for this proposed system.

## **B-2. LE-IMAGS Application<sup>9</sup>**

### ***General Information on LE IMAGS***

IMARS/FWS/RLE is a replacement only in part, for the LIER system. There are several other refuge and region-specific applications that will also be replaced with this new module.. The primary user group appears to be law enforcement officers attached to the National Wildlife Refuge System. It appears to have significant redundancy to the departmental IMARS application. LE IMAGS is a web based application. LE IMAGS is currently undergoing user acceptance testing. LE IMAGS was developed using JBOSS and a variety of development tools (VI, emacs, eclipse, and notepad). Essentially LE IMAGS is a web-based application with a J2EE architecture. It uses an open source equivalent of Macromedia's Cold Fusion or IBM's Websphere products called JBOSS. JBOSS IDE is fully integrated with the open source IDE eclipse. Currently the database being used by LE IMAGS is SQL Server, but the LE IMAGS application uses JDBC to communicate with its database thus Informix, Oracle, SQL Server 2000, or DB2 could be used for the deployment version of the application. There appear to be 3 to 4 LE IMAGS developers who are working with a group of National Wildlife Refuge System managers / users in the development and refinement of LE IMAGES requirements. Officially, LE IMAGES is billed as a module beneath LEMIS 2000, but the two development groups are separate and are using different development tools. Both applications use a J2EE architecture, but LEMIS uses Cold Fusion extensions and a Cold Fusion application server while LE IMAGES uses JBOSS. These differences could cause integration issue and could hamper component sharing between the two development groups.

LE IMAGS has some very rudimentary geospatial capabilities. A user can use an ArcIMS generated map (linked from within the LE IMAGS application) to generate Lat/Long coordinates for the location of an incident. The user simply clicks on the ArcIMS map and then the coordinates are transferred to the LE IMAGS application. Unlike LEMIS, LE IMAGS uses Active Directory for access control.

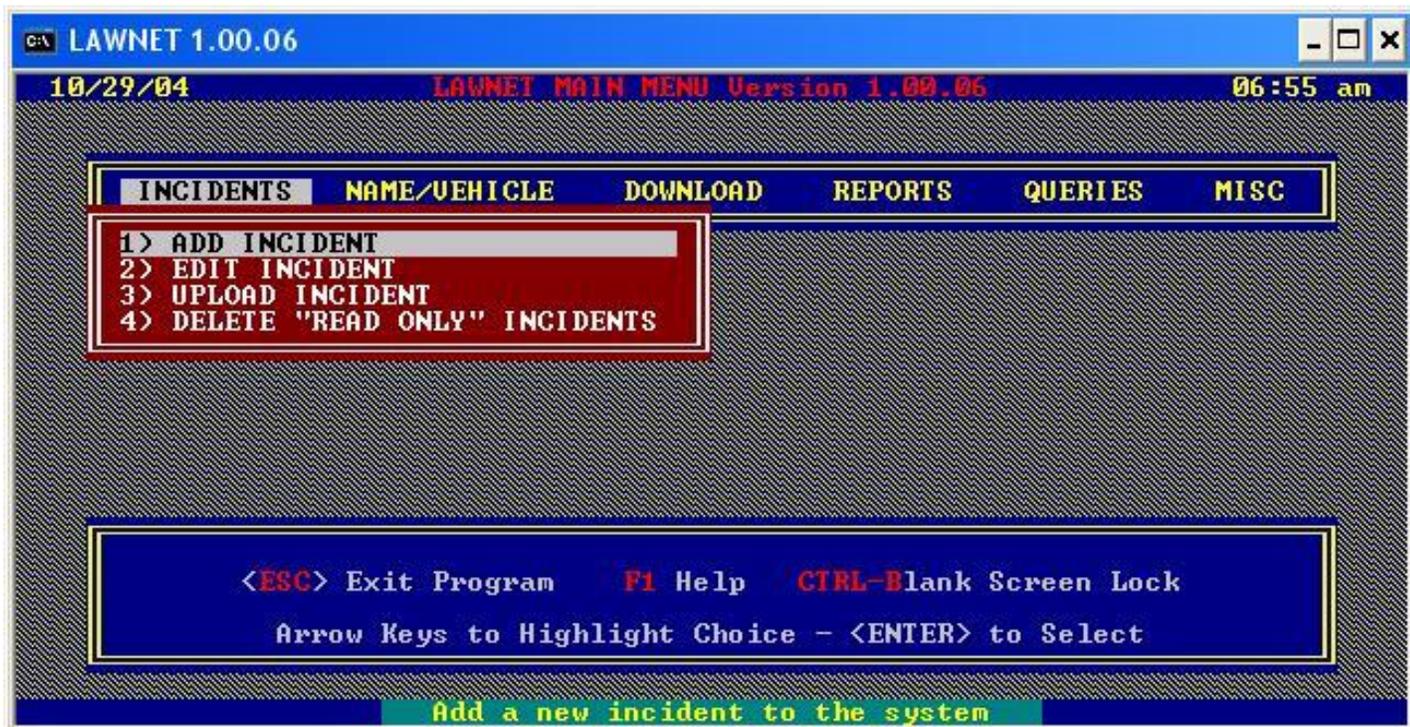
## **B-3. LAWNET Application**

### ***General Information on LAWNET***

LAWNET is a DOS / Clipper v5.3 application with links to a central Informix SQL database located in Boise, ID. LAWNET is a stand alone DOS application, but it can upload / download incident files from the central server. Client upload / download times and frequency are determined by the user. The client can also perform and retrieve simple queries against the central database. According to one user interviewed, upload and download times from the central server can be extremely long – 1 hour or more. For clarification, a typical incident in LAWNET takes about a minute and a half to three minutes to upload or download. With this in mind, an average user would take more than an hour or more per upload only if s/he uploaded incidents once every two months. If the same user were to upload once a week, each session would take about fifteen minutes. LAWNET data only goes back to 1997 or 1998. LAWNET data would need to be captured and migrated to any replacement system to allow historical reports. As of October 28, 2004, there were over 117,000 incidents on the LAWNET Server.

---

<sup>9</sup> LE-IMAGS is now a module under the LEMIS application and is referred to as IMARS/FWS/RLE internally.



*LAWNET DOS Client Screen Shot*

LAWNET is a NIBRS compliant system and is capable of generating a NIBRS report; however LAWNET does not report NIBRS data directly to the FBI. The BLM, like all other Department of the Interior subordinate bureaus, report crime statistics to the DOJ/FBI through the Department. Since the Department of Interior has yet to switch to NIBRS from UCR format of reporting, the BLM is reporting crime statistics in the UCR format even though it is NIBRS compliant. The UCR is submitted once a year around March and includes crime statistics for the previous calendar year.

There are two basic BLM user groups for LAWNET: Special Agents and Law Enforcement Rangers. Within the BLM there are perhaps 200 Law Enforcement Rangers and 50 Special Agents. Law Enforcement Rangers primarily patrol BLM lands. They perform patrolling duties, protect Federal assets, safeguard citizens, enforce criminal laws and regulations, and process violations that occur on Federal lands. This field-duty is often performed in remote regions with no access to high-speed internet or even 800Mhz radio-based connectivity.

If a Law Enforcement Ranger observes a violation of BLM enforceable criminal law or regulations, he/she may issue a violation notice (warning or ticket). Within the Patrol log Book<sup>10</sup>, there are forms for

- Incident record
- Advice or rights (Miranda Rights)
- Colorado State Patrol Impairment Examination Reports (DUI)
- Significant Activity Report
- Consent to Search
- Voluntary Statement
- Use of Force Report
- Domiciled Vehicle Use Log

<sup>10</sup> The Patrol Log Book is a bound version of primarily BLM Form 9260-15 Patrol Log and some other official forms that LEOs may commonly use in the field. The Patrol Log and other similar type forms are used by Rangers across the BLM.

Depending on the violation, various forms are filled out manually. At a minimum, the Law Enforcement Ranger has a carbon copy of the violation (From 9260-9 or 9260-10) with some added notation on the back of the ticket. After returning from the field, the Law Enforcement Ranger then logs onto LAWNET and manually inputs all incidents / violations. Some field personnel have rugged laptops and update LAWNET incident data in the field. In all cases LAWNET data input is performed after-the-fact and not in real time. The Law Enforcement Ranger must also manually follow-up on the disposition of the case. It should not be inferred that BLM law enforcement officers are “stuck” in the office because of LAWNET instead of out catching criminals. The reality is that law enforcement officers have become much more efficient as a result of the LAWNET system. In 1996, before LAWNET, the BLM reported in the UCR a ratio of 57 incidents per officer. In 2003, LAWNET data was used to report in the UCR a ratio of 92 incidents per officer. In fact, there is one ranger with 911 incidents reported in 2003. The LAWNET system was designed with a store and forward architecture so an LEO can input an incident into LAWNET while in the field and upload the incidents when back in the office connected to the Bureau’s network.

The LAWNET system is being used by all law enforcement offices in the Bureau. The BLM Law Enforcement General Order 30 and Handbook 9260-1 are very specific on the requirements to use LAWNET for reporting law enforcement incidents and what the reporting thresholds are. The rule of thumb for the Bureau’s law enforcement program is that “If it isn’t in LAWNET, it didn’t happen”. This means if an incident isn’t reported in LAWNET it won’t reflect in the UCR/NIBRS reports or be counted as an accomplishment in the Department’s MIS database. BLM officers not using LAWNET run a huge risk of losing funding due to lack of MIS accomplishments or a perceived lack of workload. Also, they are violating mandatory policy by not properly reporting law enforcement incidents and investigations. .

The screenshot shows the LAWNET 1.00.06 Incident Form input screen. The form is titled "Incident Form 0464700011" and contains the following fields and sections:

- State County**: ORI # Office
- Incident Location**: Locat Code Land Status Legal Description
- Location**: UTM-North UTM-East Latitude Longitude
- Table**: Dt Ind Incid Dt Time To Dt Time DOW Reported Dt Time Investgd Dt Time
- Ex. Clear**: Ex. Clear Dt Clear Date Time
- Actions Taken**: Subcodes Dispositions Subcodes Fine Restitution
- Method of Operation**: <Method of Operation>
- Related Incident #s**: Other Agency Inv. Cost Code
- Released to**: Released Dt
- Total**: Hours on Incident Property Value Stolen Vehicles Recovered Vehicles

At the bottom of the screen, it says "Esc to Abort PgDn when done".

*LAWNET Incident Input Screen*

Some fields within LAWNET offer pick lists and these are accessed using the down arrow. LAWNET has some work flow and data error checking. Most error checking is centered on NIBRS compliance.

The user can perform a validation check and then LAWNET provides some limited insight into the nature and location of the problem.

Special Agents occasionally perform duties similar to Law Enforcement Rangers. The Special Agent tends to perform more long term investigations and would also be more likely to be engaged in a long term case that would go to trial. LAWNET was mainly designed to support the short term needs of the Law Enforcement Ranger and not the Special Agent. LAWNET makes no distinction between a long term investigation and an incident. LAWNET does not support the adding of attachments, cut & paste, or the saving of LAWNET cases to a file or PDF format. LAWNET does have fields for capturing of geospatial data:

1. UTM Coordinates
2. Township Range
3. Latitude
4. Longitude
5. Land use and location code

But these fields must be manually typed – LAWNET does not support links to GPS data collection devices.

Special Agents has the need to perform geospatial analyses in support of court cases. Sometimes court cases require the integration of CAD drawings and GIS plots into the case file. Currently this is all done manually with occasional manual updates from the on-going case file to LAWNET. Special Agents sometimes require access to legal information (similar to WestLaw in LEMIS 2000), but no such capability is provided by LAWNET.

Seized items are tracked in LAWNET under evidence. Each inventory item is assigned a unique ID via LAWNET that is tied to the case file. The LAWNET evidence tracking system appears to be limited and no evidence disposition or tracking reports were evident.

LAWNET has its own password and user ID system. LAWNET assigns a unique incident ID based on the year, computer number, and the incident number. For example the second case by computer 218 for 2004 would be:

*0421800002*

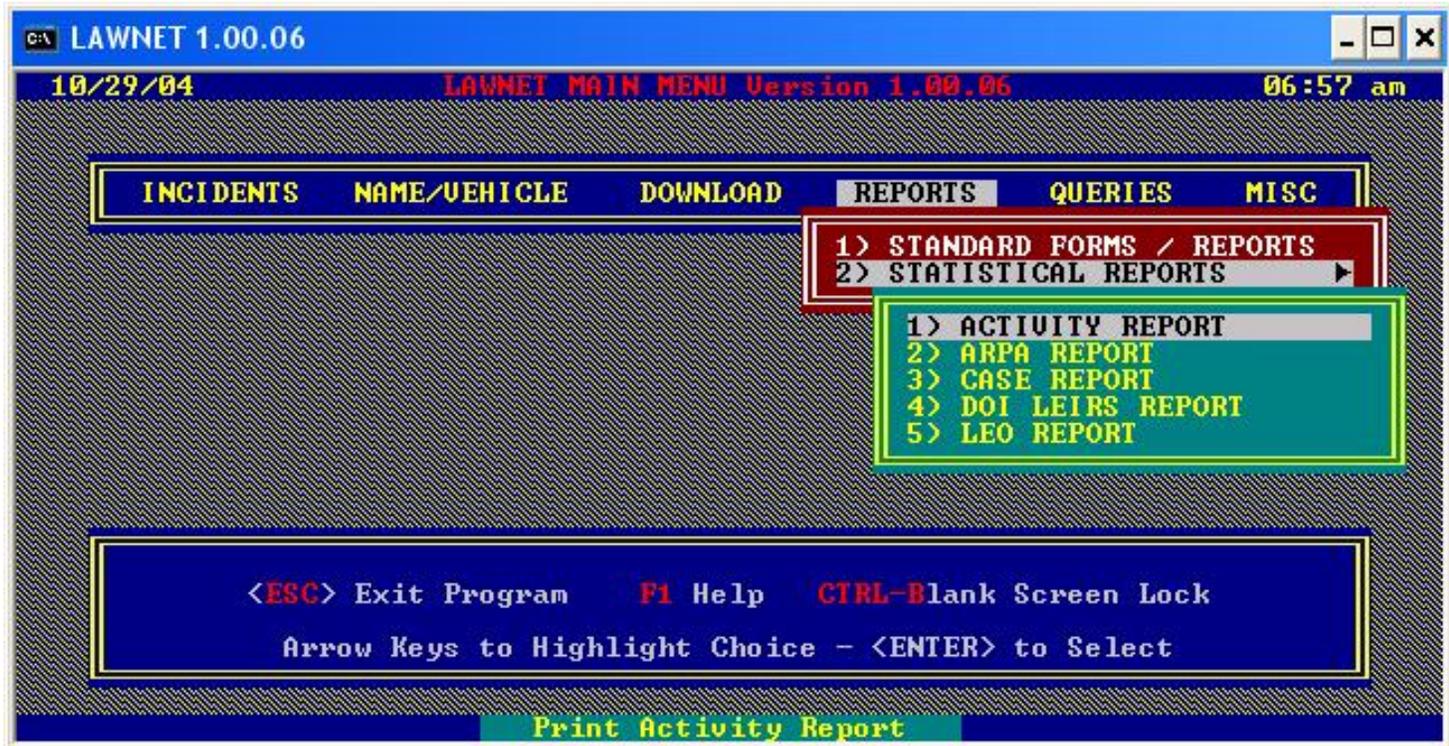
With LAWNET a user can be the investigating officer, an assisting officer, and an approving officer. Cases can be flagged as internal affairs, confidential, or be given a red flag indicating something like a dangerous criminal. If tagged as internal affairs, only the investigating officer and designated assisting and approving officers can read the file. This flag never expires. If tagged as confidential, it's essentially like internal affairs but expires in 60 days unless renewed. Red flags have no restrictions. Any LAWNET user can download and read an incident file as long as it is not tagged as internal affairs or confidential.

LAWNET collects certain time and reporting information. LAWNET requires a cost code (a.k.a. BLM program element code) to complete an incident form. This cost code does not directly correspond to the hours charged against a given accounting code in Paycheck. The cost codes represent actual work performed whereas the Paycheck application recording represents allocated funding. There are rarely in agreement.

LAWNET allows for certain simply queries. Queries against the central (or Master) server required a dedicated internet / LAN connection. Typically, LAWNET users download only a very limited number

of incidents onto their local systems. Local searches are limited to the extent of the downloaded data. Users may query for names, vehicles, or against fields within LAWNET

LAWNET has limited reporting capabilities. There is essentially one LAWNET report where the user can select to print the complete report or merely sections of the incident. There are also a variety of statistical reports.



### *LAWNET Report Capabilities*

#### *BLM Law Enforcement LAWNET Replacement Requirements*

1. Current LAWNET field users capture data manually. Ideally, field users should have some field data collection device that captures initial incident data, prints a BLM Form 92601-9 or 9260-10, and then syncs with the central server on a regular basis. If a field device still requires manual capture and printing of a violation notice, then it will duplicate efforts. It needs to be emphasized that field personnel currently spend close to 20% of their time re-typing incident data into LAWNET. The vast majority of this incident data could have been captured at the source. An ideal field data collection device would also have GPS capability. Currently field coordinates must be typed in manually after the fact.
2. The DOI must carefully consider the needs of BLM and other bureau field personnel when selecting the architecture for a LAWNET replacement. Other DOI incident management systems such as LE-IMAGS are web-based J2EE-compliant applications. LE-IMAGS does not support a disconnected environment, but would be ideally suited to the needs to law enforcement personnel who have access to an adequate TCP/IP connection to the central server. There are ways to architect and implement J2EE-compliant applications that work in a disconnected mode. Another approach would be to have a field data collection device / application and a web-based LAWNET replacement application. Certain companies have Windows CE and Palm OS

software which support law enforcement activities<sup>11</sup>. Other companies have created robust public safety software solutions that support wireless devices<sup>12</sup>.

3. BLM law enforcement personnel will be direct users of any LAWNET replacement. Unlike FWS personnel who have legal administrative assistants to input / validate incident files, BLM law enforcement personnel work directly with LAWNET with limited support. Any LAWNET replacement must be user friendly, have adequate built-in data validation and type-checking, and have context-sensitive help.
4. The Current LAWNET application does not differentiate between simple violations and long term investigations. Ideally, the LAWNET replacement should distinguish between the Law Enforcement Ranger and Special Agent user groups.
5. The current LAWNET application is a DOS client and is several years beyond its original projected life time. Since it was implemented more than 10 years ago using Clipper, it requires considerable re-engineering every time a new version of Windows is deployed at BLM. Any LAWNET replacement should have minimal client-side requirements / dependencies.
6. Currently, roll up from client to server is not automated, thus some users will update daily while others may only update monthly (or when they feel like it). Replication should be quick, automated, and scheduled on a regular basis.
7. Currently the reporting module is limited. LAWNET does have some Informix stored procedures for regular reports (including NIBRS), but ad hoc reports require custom querying and capture of output. Ideally, a LAWNET replacement should support robust SQL-based reports and geospatial queries and reports.
8. Currently, the only access supported is either console (tied to a given computer) or dial-up. No Internet access is allowed.
9. Currently attachments such as digital photos, documents, scanned images/documents, and URLs can not be linked to an incident file. This is a serious short coming of LAWNET that should be addressed by any replacement system. LAWNET reporting does not created a case report suitable for legal prosecution.
10. BLM law enforcement personnel often collaborate with other State and Federal law enforcement personnel. The LAWNET application does not support incident case sharing. The BLM may wish to investigate Forest Service law enforcement applications. In many situations, Forest Service and BLM personnel are co-located and share responsibilities. BLM, for example, is responsible for law enforcement activities associated with sub-surface minerals and oil & gas on all Federal lands including National Forests.

### ***Detailed LAWNET System Specifications***

#### Client Application

- Clipper version 5.2e

#### Client DOS communication library

#### COTS

- Clipper Tools version 3.0
- Blinker version 3.10
- Six Drivers version 3.1

---

<sup>11</sup> <http://www.cybercop-software.com/>

<sup>12</sup> <http://www.visionair.com/>

- Novlib version 3.10
- Esc40 version 1
- ClassY version 1
- Llibca version 1

Written by PSI

- minh (Minh Tran library)
- mwizard (Minh Tran library)
- madhoc (Minh Tran library)
- hplib (Harry Patton library)

*ABC elements automated (fully or partially) by the LAWNET system*

In 2003, the Bureau's annual targets were set and input into MIS by our office (Office of Law Enforcement and Security) for the Program Elements (PE) **NL**, **NN** and **NO**. The the LAWNET System then calculated the actual accomplishments for these same PE's. Inputs of accomplishments for these PE's were not allowed from any other source. The Bureau made some major changes to the Program Elements (PE) starting in FY2004. Since this change, LAWNET now calculates and reports accomplishments for the PEs listed below. The PEs NL, NN and NO no longer exist in MIS. Also, because of the wider range of PEs support that are no longer law enforcement specific, LAWNET isn't the only source of input of accomplishments.

**AL - Provide outreach through interpretation and environmental education**

**EB - Issue and Manage Recreation Use Permits**

**EG - Prepare Vegetative Permits/Contracts**

**HF - Restore and Protect Cultural/Paleo Properties**

**HO - Respond to Hazmat Risk Sites**

**HT - Ensure Fire Preparedness**

**HU - Suppress Wildland Fires**

**NA - Inspect Grazing Allotments for Compliance**

**NB - Conduct Fluid Mineral Inspection and Enforcement**

**NF - Inspect and Verify Production at Mineral Material Sites**

**NG - Inspect and Verify Production at Solid Mineral Sites**

**NH - Conduct Realty and Geophysical Compliance Inspections**

**NI - Inspect Locatable Mineral Sites for Surface Management Compliance**

**NJ - Process Trespass/Unauthorized Occupancy Cases**

**NK - Conduct WH&B Compliance Inspections**

**NU - Conduct Patrol Enforcement Activities**

**NV - Conduct NonDrug Investigative Activities**

**NX - Inspect Commercial SRPs for Compliance**

**NY - Conduct Emergency Response Activities**

**NZ - Conduct Security Activities**

**OA - Conduct Drug Enforcement Activities**

**PN - Provide Program Support: Protection of Lives, Resources and Property**

## Appendix C – Glossary of Terms

Name	Description
ABC-WORK-ACTIVITY	Activity Based Costing (ABC) is a management process that examines how program activities consume resources and produce outputs. In ABC, work processes are broken down into activities so that the cost and performance effectiveness of the activities and processes can be measured. The ABC-Work-Activity object describes an activity that can have work tied to it to measure effort against.
BUSINESS-AREA	An FEA BRM Business Area as defined by OMB.
DATA-SUBJECT-AREA	A broad classification of information or a grouping of related entities (those in which data are closely related and describe a general business idea or object) are called Data Subject Areas (DSA). A DSA is a grouping of entities based on a commonality of the data, and NOT how it is used by any given business process or application.
END-OUTCOME	End Outcomes (EO) are long term performance goals which describe and support the DOI's strategic goals. End Outcomes express a desired result and are measured by one or more performance measures / indicators. Performance measures indicate the success in achieving the long-term goal.
END-OUTCOME-MEASURE	A measurable indicator of the End Outcome that can be systematically tracked to assess progress made in achieving predetermined End Outcome goals and using such indicators to assess progress in achieving these goals. A measurement must be an Operational Measurement Indicator in the Mission and Business Results Measurement Area. The Operational Measurement Indicators agencies create should be determined by referencing the End outcome indicators identified in the DOI Strategic Plan. A Measure must fit within the three Measurement Categories of the Mission and Business Results Measurement Area of the PRM. These categories are Services for Citizens, Support Delivery of Services, and Management of Government Resources. This Measurement Area aligns with Measurement Areas described in the Business Reference Model Version 2.0.
FUNCTION-ACTIVITY	BRM-TIER represents an entity in the FEA BRM. A BRM-TIER can be a Business area, Line of Business, or Business Sub Function or a further Agency specific decomposition. It is the super entity for BUSINESS-AREA, LINE-OF-BUSINESS, SUB-FUNCTION, LEVEL-2-SUB-FUNCTION, WORK-ACTIVITY, and PROCESS-STEP.
INTERMEDIATE-OUTCOME	Intermediate Outcomes describe and support major milestones of an annual End Outcome goal. There are two or more Intermediate Outcome Goals to every End Outcome Goal. The actual results, effects, or impacts of a business initiative, program, or support function. Actual outcomes typically are compared to expected outcomes
INTERMEDIATE-OUTCOME-MEASURE	A measurable indicator of the Intermediate Outcome that can be systematically tracked to assess progress made in achieving predetermined End Outcome goals and using such indicators to assess progress in achieving these goals. A measurement must be an Operational Measurement Indicator in the Mission and Business Results Measurement Area. The Operational Measurement Indicators agencies create should be determined by referencing the End outcome indicators identified in the DOI Strategic Plan. A Measure must fit within the three Measurement Categories of the Mission and Business Results Measurement Area of the PRM. These categories are Services for Citizens, Support Delivery of Services, and Management of Government Resources. This Measurement Area aligns with Measurement Areas described in the Business Reference Model Version 2.0.
INVESTMENT-PROJECT	The INVESTMENT-PROJECT model object captures both information technology-related investment and project information. An IT Investment represents a special type of capital project (or investment). An Investment for an IT project has a corresponding Exhibit 300 and is represented by a summary line on an Exhibit 53. A Program may sponsor many Investments, but an Investment may only have one sponsoring Program. Many Programs, however, may support an Investment by contributing funds, and a Program may support many Investments.
LINE-OF-BUSINESS	An FEA BRM Line of business. The LINE-OF-BUSINESS inherits attributes from BRM-TIER. The complete As-Is DOI Business Architecture for the following business areas: Fire Management, Law Enforcement, Finance, Recreation etc....
MISSION-AREA	This is the goal level used in bureau and office plans, sometimes referred to as the mission goal level in bureau plans. This level is not directly measurable. Interior crosswalks budget activities to the GPRA program activity level.
SERVICE-COMPONENT	The final layer of the SRM is the Component level. These 168 Components represent the lower-level, logical "building blocks" of a business or application
SERVICE-DOMAIN	The Customer Services Domain defines the set of capabilities that are directly related to an internal or external customer, the business' interaction with the customer, and the

Name	Description
	customer driven activities or functions. [REF: FEA_SRM_Release1.0]
SUB-FUNCTION	An FEA BRM Business SubFunction. SUB-FUNCTION inherits attributes from BRM-TIER.
SUB-SYSTEM	Subsystems are used to refer to groups of applications or components that form part of the system. A subsystem is a logical organization for a solution and is not directly deployed on the technology infrastructure.
SYS-COMP/DEPLOYMENT-INSTANCE	This associative entity will be implemented as a matrix (or other means to be determined) in system architect to resolve the many to many relationship between PROCESSING NODE and SYSTEM-COMPONENT. It describes how a SYSTEM-COMPONENT is deployed on X,Y,Z...PROCESSING-NODES- When, How, and the Architecture Tier (Web, Network, Application, Database).
SYSTEM_	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. [JP1] An IT system is a combination of hardware, software and documentation that implements and describes a solution. A system is the top-level organization for a solution and is not directly deployed on the technology infrastructure.
SYSTEM-COMPONENT	System components are used to describe the constituent bits of functionality from which the system has been assembled. A system component has the following three characteristics: 1) It is a modular unit of functionality; 2) It is logically isolated from other system components by making its functionality available through defined programming interface boundaries and may use other component interfaces; and 3) It is associated with a processing node and is actually deployed on the technical infrastructure (as opposed to systems and subsystems which are containers or collections that are not directly associated with a processing node).