BA FINDINGS AND RECOMMENDATIONS

The following pages are a compilation of findings and recommendations from the Summary Report of the Initial Bureau Architecture (BA) (Bureau of Land Management, March 31, 2000). For explanation of these extracts, refer to the appropriate section of the BA Summary Report, indicated in square brackets after each paragraph.

OVERVIEW OF BA RECOMMENDATIONS

BA recommendations concern the following major areas:

< immediate implementation strategies for information technology (IT) and business investments to both improve the current architecture and begin the migration to the future architecture.
< recommended architectural criteria to be used by the IT Investment Board (ITIB) to judge whether both existing and proposed IT projects fit the future architecture.
< structures to use and maintain the architecture into the future.
< a suggested order of implementation.
< a description of what additional work remains to be done to build out the rest of the BA.

[Section 1]

IMPLEMENTATION STRATEGIES

In this report, the BA Team has grouped actions into six implementation strategies. These strategies are:

> **Facilitating the Accomplishment of BLM Work in the Field**–*Delivery of Information Directly to the Program Specialist/Decision-maker*
> **Improving the Utility of BLM Business Processes and Information**– *Making Sustainable Resource Decisions; Replacing Out-dated Land Use Plans*
> **Managing BLM's Information Resource is Part of BLM's Real Work**–*Establishing Accountability, Responsibility, and Authority*
> **Assuring and Storing High-Quality Program Information**–*Structured Data Administration and Management*
> **Providing the Solid Foundation on Which All Technology Works**–*Infrastructure, Network and Security*
> **Getting the Return on Investment and Budget Dollars**–*Management of Information Technology Investments*

[Section 3.1]

Project Selection Criteria Relative to the BA

The following Initial BA criteria are recommended for use in reviewing new projects and proposals, and for periodic assessment of existing systems. These criteria address only the issue of conformity with the BA.

1. **Module Building Toward the Desired Future BA.**
   Existing and proposed IT investments or continued support of in-progress projects must demonstrate that they contribute modules which align clearly with the authorized BA and contribute directly toward attaining the desired future BA concepts. Those projects which deal with the "crisis of the month" must be made to migrate toward the desired future BA. In this context, the ITIB is responsible for making the "keep-toss-acquire" decision in evaluating new proposals or in reviewing the IT BA. As used here, the term 'acquire' is defined as the full spectrum of acquisition—from developing in-house to full out-sourcing.

2. **Attaining the Process-Based Orientation.**
   Existing and proposed IT investments that are "stovepipe" will not be deemed as architecturally compliant and new applications must seek to address "cross-cutting" process functionality as defined in the current authorized version of the BA. Support for the BA will be accomplished by further defining and detailing (to levels 4 and 5) the initial version BA work processes and then utilizing, augmenting or replacing existing process-oriented applications and/or buying/building new process oriented application(s) if not already existing. Proposals will be supported by specified PDAT information, which is directly relatable to the PDAT elements of the BA.

3. **Enhance Operational Efficiency – Store Data Once.**
   Databases will be owned and maintained as resources distinct from the applications that use them. New projects (including acquisition of purchased applications) will not build or create redundant primary store data entities when there is an existing primary data store that already contains that entity. Secondary data stores may be appropriate in some situations for performance and security reasons; however they may not be used as a redundant mechanism for storage of identical data. Data will be created, updated, maintained, and retired only once through the primary data store. New projects must either utilize the existing primary data store, or seek to fully replace the existing primary data store and support all other existing applications that rely upon it.

4. **Preference for Use of Established BLM Technology**
   Existing and proposed IT investments or in-progress projects must not require the introduction of new types of technology infrastructure (including standards and protocols) beyond those identified in the future (desired) portion of the current approved version of the BA. Any requirement for new technology must first be incorporated into the BA, through an orderly process, before being introduced into new or existing applications.

(This includes both strategic existing and missing strategic technology components.) Also, projects and proposals for new applications or in-progress projects will not be architecturally acceptable if they require significant investment in augmenting or modifying technology infrastructure components which have been designated for retirement or replacement.

[Section 3.2.2]

REFINING AND MAINTAINING THE BA – ANTICIPATED FUTURE EFFORT

1. Further Analyze High Level Data Entities and Primary Business Subject Areas

The BA has identified over 30 high level data entities or groups of related information. Some of these entities, for example Land Status and Customer, are used by a many different processes throughout the BLM. These areas are defined to the third level business processes with closely related high-level data entities. Based on the priorities identified earlier in this document, the process BA will need to be further defined to the appropriate level to support data modeling and system development. The benefit of this effort would be to provide a common business understanding for the applications and databases required to support the business subject areas.

2. Work with Project Teams to Ensure Maintenance of the BA

As project teams develop new applications and databases are developed, and enhance and modify existing applications and databases, they will provide additional information about process, data, applications and technology. This information should be incorporated into the BA so that it accurately reflects the BLM's current status and future vision. The benefit of doing this would be to have one central place that captures the BLM's processes, data, applications, and technology, both current and future. This process is essential to maintaining the BA and guiding investment decisions.

3. Develop BLM's Current Application Inventory

Twelve of the BLM's applications were analyzed as part of the BA effort. This is a small sample of the total applications that the BLM uses. The purpose of developing BLM's current application inventory would be to assess each major application that the BLM uses in terms of its usefulness to the business community, how easy the system is to run and maintain for the IT community, and how well the application fits into the BA. The benefit of this effort would be that the BLM would have a better understanding of its application inventory, would be able to identify systems that need to be replaced because they don't meet user needs or are hard to maintain, and would be able to identify redundant and best-in-class systems. The level of assessment required will be a judgement call based on how the application does or does not support the current business needs. Implementation of an Enterprise Management System (EMS) would facilitate the process.

4. Interface the BA Components into BLM's Corporate Meta-Data Repository

Currently, most of the BA is represented in the form of business models in Cool:Biz®. However, within NIRMC, there is a Corporate Meta-Data Repository (CMR) which serves as the repository of information about the business processes, data, systems, databases, etc. that support BLM. The information currently in the Cool:Biz® repository should be available to the CMR. The benefit

of this effort would be to make all information about the BLM that has been gathered about BLM available in from single source – the CMR. However, since the CMR does not support all of the information and functionality contained within the Cool:Biz® repository, the information currently in the Cool:Biz® repository will be maintained there as well.

5. Update the BLM BA Internet/Intranet Site

The information contained in many of the diagrams and reports that make up the BA is only available in hard copy and on LAN-based files. The intent of this effort would be to make the information contained in the BA available to anyone who wants to look at it through the Internet/Intranet. This would reduce the amount of effort needed to respond to people wanting copies of all or part of the BA.

6. Determine the Current Status of Technologies within the BLM

A more pro-active examination of the rapidly changing technologies, including Internet, database design, and GIS needs to occur to provide guidance in the development of the BA. The BA has a snapshot of the technologies currently in use by the BLM, including hardware, networking, and fundamental IT services that support data and applications. We also need a more comprehensive understanding of the availability and use of technology in the BLM. For example, throughout the analysis it was clear that Geographic Information Systems (GIS) can provide support to the business processes and information needs of the BLM. Some offices use GIS extensively; others use it infrequently. The purpose of this effort would be to find out how GIS is being used throughout the BLM. By doing this, best practices for the use of GIS could be identified. Further, rather than reinvent the wheel, perhaps some of the GIS software already available could be used to meet the needs of other BLM offices.

[Section 3.3.1]

INCORPORATE THE BA INTO THE BLM'S DECISION PROCESSES – ESTABLISH A FULL-TIME CAPABILITY TO MANAGE THE BA

1. Establish a BLM Entity to Manage and Facilitate the Use of the BA

A Business Architecture Office (BAO) should be established, as proposed by the BA Team, would report to the BLM Deputy Director and Assistant Directors and the mission Assistant Directors (200, 300, 800) . It would be responsible for the refinement, enhancement and maintenance of the BA, and especially the Business BA components. The BAO would work with the BLM managers and program specialists to define business needs, conduct associated business process analysis, support the development of data standards, and support improvement of data quality. The BAO would also provide BA support to project sponsors, analyze, and review proposals and approved projects, similar to the CIO's staff, but more from a business viewpoint.

The CIO has a proposed IT Coordination Office to provide the principal support to the ITIB, supporting and coordinating with the BAO and NIRMC. The IT Office would also support the BA by maintaining the BA repositories (e.g., Cool:Biz®, CMR, etc.), leading the data modeling and derivation of application and infrastructure requirements, and providing contract support for the BA. Working with the BAO, the CIO's staffs would then derive data models, application functional requirements, and determine impacts on technology requirements to implement the BA. The IT Office will provide managers of IT projects with management standards, guidance, and support on project proposals and approved projects.

2. Institutionalize BA as Part of BLM

Now that the BA has been developed, it is important that it be made part of the BLM's decision-making and system development processes. This requires training and educational steps that work to ensure that the ELT, ITIB, senior management, and staff of the BLM understand the BA and are connected to using it as a decision support tool.

3. Ensure that All Applications Being Implemented Conform to the BLM BA

The BA describes the desired future for our business processes, data, applications, and technology and a path to get there. Only those applications that conform to this path should be built or acquired.

[Section 3.3.3]

PDAT CONSOLIDATION

The following findings are the most important emerging from the PDAT analyses.

< The BLM has no effective assignment of ownership of business processes, data, applications, or technology infrastructure. Consequently, there is no clear accountability for successes or failures. Commonly, there are competing and uncoordinated deviations from, and modifications to "standards" across the BLM. "Effective ownership" must include assignment of each BA component to one named individual; granting that individual undivided control of that component; providing real rewards and sanctions for performance by the individual; and providing sanctions against any infringements of that owner's prerogatives by any other BLM personnel. *Single-point ownership does not necessarily imply centralization at the national level.* BA components should be "owned" at whatever level of the organization is most appropriate–taking into account legitimate differences among jurisdictions.

< There is no complete, up-to-date, and reliable inventory of business processes, data sets, computer applications, or IT infrastructure components (including standards and protocols). There is consequently no current basis for the "IT Investment Inventory" required by the ITIB to evaluate investment decisions, and thus BA implementation is handicapped. Configuration control and IT contract management are likewise inhibited.

< There is not yet in place a complete IT investment management system, consistent with the Clinger-Cohen Act and OMB guidance, by which all further IT investments made anywhere in the BLM are to be evaluated by objective criteria and procedures. This includes prioritizing investments in relation to priorities of the BA. At present, program funds are routinely applied to IT investments, out of view and out of the control of any collective IT decision process. Investment procedures are not, strictly speaking, part of the BA, but must be in place for it to succeed. Steps are underway to fill this gap.

< Powerful structural influences have encouraged "stove-piping" of business processes, data sets and computer applications. The BLM manages and funds major programs almost as if they were separate, and sometimes competing, lines of business. This stove-piping of programs (the "vertical" or "org chart" view of the organization) inhibits more logical organization of work around common business processes shared by the programs–forcing a high degree of process duplication among the programs. Stove-piping of funding strongly encourages stove-piping of applications development and duplication of data sets to support the stove-piped applications.

< A very high percentage of all BLM business processes involve, or should involve, access to tabular documents and geospatial information, on the same screen, easily accessed, reliable, and internally consistent. The current BLM approach to GIS and geospatial data tends to isolate GIS in small groups of GIS specialists, who provide map-making and analysis support to the program staff on a pay-for-service basis. This approach separates

the end user from the tools, data, and skills they need in order to use geospatial information as an integral, routine step within their daily business processes. This approach to GIS as a separate business process in its own right is also an impediment to proper technology infrastructure planning, since geospatial technologies require major accommodation for storage and data transfer.

< Data design and management practices, whether viewed at the detailed technical level or the corporate management level, are highly inconsistent, and do not typically conform to industry best practices. The BLM's data resource is commonly understood to be critical to its business, but that resource is a very long way from being complete, controlled, up-to-date, reliable, or even inventoried.

[Section 4.1.2]

The analysis of the BLM's processes and information requirements resulted in the identification of the following Business Subject Areas:

< Guidance
< Land Use Planning
< Authorization and Enforcement
< Compliance and Monitoring
< Land Status/Resource Condition Determination
< Records Management
< Name and Address Management
< Work Management
< Administration

These business subject areas are high-priority candidates for possible additional, cross-program automation support.

[Section 4.1.3]

4.1.4 Implementation Plan and Staging–Consolidation of Major PDAT Recommendations

The following table presents the consolidated PDAT implementation steps and stages resulting from this analysis to date.

Stage	All Components	Process	Data	Applications	Technology
1	Create/maintain accurate inventories of PDAT [6, BA] Define, then assign ownership to each PDAT component [3] Improve IT investment management practices. Ensure all proposals (changes to existing and new) are aligned to the BA. [6] Refine and maintain BA PDAT and priorities [BA]	Refine future business process model [BA] Place models under strict configuration control [BA]	Implement technical data management improvements (see Section 4.3) [1, 2, 4] Employ relational database technology tools to enforce business rules[1, 2, 4] Separate data from applications [1, 2, 4] Place the data resource under comprehensive management control [1, 2, 4]	Name an enterprise-wide applications coordinator [3] Implement technical applications design recommendations (see Section 4.4) [BA] Establish single BLM-wide accepted list of mission critical and essential applications. [6]	Implement ‹Security in Depth’ Technology Architecture as part of BLM response to DOI-NET FY2000 network reconfiguration effort. [5]

Stage	All Components	Process	Data	Applications	Technology
2		Implement BP change management process [6] Begin to incorporate GIS into business processes [1, 2]	Complete logical data models for all existing systems and perform a gap analysis against the enterprise data model [4] Integrate enterprise data model with Corporate Metadata Repository [4]	Refine process and information flow requirements into clearly defined production environment performance metrics. Establish corresponding Service Level Agreement (SLA) for all production applications, and, as part of the proposal for all new applications. Start with mission critical first. [1, 5 , 6]	Reconfigure and deploy existing / new Technology components to support multi-purpose use and augment contingency / business continuity. [5]
3		Extend process models to level 5-6, as required, as part of specific proposals and initiatives [1, 2] Apply business process modeling lessons in future organizational re-alignments [6]	Manage data as a corporate resource; create enforceable management structures and apply resources to ensure that data are accessible, current, reliable, and secure [3, 4, 5]	Coordinate geospatial projects above state office level as appropriate to the topic. [1, 2, 3, 4, 5]	Develop/Implement robust monitoring mechanisms to track and report to Process Owners actual performance relative to SLA desired metrics. Use performance information to develop trends and overall Technology Infrastructure investment requirements. [5]
[ ] Key:		BA Required for BA Implementation 1 Delivery of Information to the End User 2 Planning Automation 3 Accountability, Responsibility, Authority		4 Data Management 5 Technology Infrastructure 6 IT Investment Management	

Table 4-1 Consolidation of Implementation Plan and Staging

4.2 BUSINESS PROCESSES

Findings

A review of the current environment (based on ABC) revealed that there are an excessive number of redundant processes. Across the enterprise 37% of all processes appear to duplicated in separate program elements.

The review of the business processes has shown an overwhelming potential for using geospatial data. Two conclusions may be drawn from this review. The first is that geospatial analysis is needed to support multiple business processes. The second is that there are a number of report generating activities which would benefit from geospatial support.

[Section 4.2.2]

Recommendations

The following list presents recommendations for actions to achieve the future business process state objectives:

Stage 1

Continue analysis of the future business model: This should be done by applying the same criteria used for analysis of both the current and future environment models contained in this report.

Assign ownership/stewardship: This is necessary for control and accountability of business process re-engineering and automation. It is particularly important to ensure that such stewardship is not ambiguous, for example, shared between program and state administrations or other organizational components.

Stage 2

Implement business process change management: This will require a change control methodology that promotes transition from current to the future desired business process model, in actual everyday practice. The change management system must be flexible enough to foster desirable change, yet sufficiently strict to prevent unauthorized changes not approved by the business process owner and BLM management.

Focus initial re-engineering on data management process: Improvements made to data collection, storage, and access will have a positive, cascading effect upon all other processes.

Fully integrate the use of technology into business processes: In all business process re-engineering activities, include a fully integrated analysis of the role of technology, such as

geospatial visualization and analysis, in the identification of business processes and information flows.

Stage 3

Complete process modeling to level 4, 5 or 6: This level of detail is required to reveal reusable process modules and enterprise information requirements. Refinement should occur as part of continuing assessment of new initiatives or project proposals.

Identify and document business rules: These support business processes and must resided within a software tool to make maintenance and user access readily available. The BLM has documented many of its business rules in detail for previous projects, but they are not in a practical repository to promote widespread reuse. This is needed to thoroughly understand the interrelationship between data and its utility within a process. Business rule documentation can be accomplished as part of developing new initiatives and projects in high-priority business areas.

[Section 4.2.2]

4.3 DATA

Findings

The analysis of current applications indicates:

< Absence of pro-active data management
< Potential redundancy in both processes and data
< Limited sharing of data or cooperative efforts to obtain commonly needed data including geospatial data
< Conformity to Federal Geographic Data Committee standards for geospatial data has been mandated and BLM is lagging behind other agencies.
< Geospatial data is always or sometimes required in 74 percent of data flows identified in the third level business process modeling effort. Much of this currently is paper information. However, at an increasingly rapid pace, BLM may expect that these data flows will be automated, with transfer of standardized digital geospatial data between a high percentage of all BLM business processes.

[Section 4.3.2]

Recommendations

The following list presents initial BA recommendations concerning the grouping and order of performance of recommendations concerning business data. This order is established purely from the perspective of improvements required to business data, without consideration of the competing priorities from the analyses of processes, applications, and IT infrastructure. The consolidation of these is presented in Section 4.1.

Stage 1

Implement the detailed recommendations for data management (see below).

Assign accountability and control of databases and data elements, per the "ownership" implementation strategy

Employ relational database technology features to enforce business rules, rather than embedding business rules in application code

Separate, for management purposes, data resources from the applications that draw upon them. This makes it possible to manage data as a corporate resource, to consolidate redundant databases, to assign and enforce responsibility for data sets, and to minimize the costs of maintaining key data.

Stage 2

Refine and maintain the Enterprise Data Model as the BA progresses through its next steps

Complete logical data models for applications as they are replaced and perform a gap analysis against the Enterprise Data Model

Integrate the Enterprise Data Model with the Corporate Metadata Repository

Stage 3

Manage data as a corporate resource; create structures and apply resources needed to ensure that data are accessible, current, reliable, and secure.

[Section 4.3.2; see end of this listing for detailed technical recommendations derived from data analysis and referenced above.]

4.4 APPLICATIONS

Recommendations

Stage 1

Conduct a BLM-wide inventory: The BLM has no complete, up-to-date, or reliable inventory of applications and there are a number of different existing application inventories that are inconsistent with each other. An effort to complete the inventory for the remaining national applications should be undertaken first, then completed based upon the prioritized Business Subject Areas. A rigorous process to keep the resulting application inventory current must also be implemented. A direct result of not having a current application inventory is it is impossible to determine where scarce IRM resources are being expended in development and maintenance, except for a few key systems at the national level, thus the BLM cannot currently execute its responsibility under the Clinger-Cohen Act to ensure that new IT investments do not duplicate existing software.

Name an enterprise applications coordinator: As previously mentioned much of the basic information regarding current applications is either non-existent or not easily found. This situation cannot be remedied without clearly named owners/co-ordinators. Also in those situations where coordination roles, administrative titles, duties, etc. currently exist they are inconsistent across various BLM programs, geographic locations, and organizational units. These owners/co-ordinators would then be responsible for tracking the applications as significant resource investments and corporate assets.

Implement the future state Application objectives: The following list provides a set of overall design guidance for all major application enhancements, new application development and COTS applications acquire/purchase evaluations:

- Applications should be designed for platform independence.
- Applications should be modular in design, with a bias toward developing major portions of them as reusable components.
- Applications should be designed in regards to push and pull technologies to take advantage of client/server technology, middle-ware messaging and deployment to the web environment (Intranet/Internet).
- Applications should conform to a single graphical user interface standard.
- Applications should be mapped to the technology tiers, future business processes and data.
- Applications must not be designed to treat the data associated with it as being solely owned/controlled by that application.
- Applications should be designed from the future BSA perspective. (process / data grouping). The current approach of acquiring / building applications at a specific BLM Program level results in widespread duplication of software components to

support a large number of business processes that are common to many, if not all, programs.

Stage 2

Define Performance Requirements for Applications: This work will refine process and information flow requirements into clearly defined application performance metrics. These performance requirement metrics as defined by the Process owner/sponsor will result in a detailed Service Level Agreement (SLA) for each production application. These SLAs need to be developed as part of the proposal for all new applications. The work should start first with the BLM mission critical applications.

Stage 3

Coordinate geospatial application efforts above the State Office Level. In some cases the States resist this but in other cases they look for it. This would help coordinate ongoing efforts in the states and find/implement best capability/least cost solutions. This includes the Beta Testing of GIS software. The current testing situation is fragmented and lacks a mechanism for communicating the problems and bugs found in the new releases of the software. There is a real need within BLM for a larger community involvement in testing the functionality. This would also reduce the individual burdens.

[Section 4.4.2]

4.5 TECHNOLOGY INFRASTRUCTURE

Findings

< In general, information on the various kinds of hardware and software in the field is substantial but incomplete. Information on the quantities of many infrastructure components is mostly lacking.

< As web enabled, and 2-3-tier and thin client applications become more prevalent, the network dependence becomes an increased availability factor.

< Current bandwidth capacity needs to increase significantly, particularly with Vendor and COTS increased adoption of n-tier architecture approaches, thin-client applications, graphic intensive applications and other large file and data transfer needs on this rise.

< BLM IT staff has an attrition rate of in excess of 12% per annum; staff departures to the private sector is a high risk, a significant percentage of BLM staff is within 5 year of retirement. Knowledge capture /Management (KM) is particularly important within the BLM, as staff retires, and incentives to join Civil Service are decreasing. Providing corporate knowledge to remaining staff in a format that can be readily accessed and assimilated, is critical to reducing the impacts of "brain drain".

< IT labor shortages, as well as budget reduction trends are causing organizations to focus on core expertise, move toward outsourcing solutions to address a wide variety of technology issues such as: non-mission critical help desk operations, office automation suites, desktop platforms, etc. The current BLM IT infrastructure is not well suited to accommodate this trend.

< The widespread (but not exclusive) use of Informix RDBMS in the BLM is a hindrance to GIS Technology progress, because currently the BLM's standard GIS software vendor is relatively slow to release the Informix version of its new software versions.

[Section 4.5.2]
Recommendations

< Reduce unnecessary redundancy in all levels of technology infrastructure components to improve efficiency and reduce costs. Ensure major technology infrastructure components particularly those of supporting multiple purposes are treated as a corporate level assets and configured to allow for/support a wide variety of needs.

< Support and encouragement for a wide variety of remote computing/intranet/web-based/wireless access and delivery needs must be considered early in the design phase of all future Technology infrastructure components.

< A similar 'look and feel' for all technology infrastructure components directly accessible by humans must be established and maintained to reduce training costs, improve productivity, support sharing among organizations, etc.

< Provide / augment protection from unauthorized or inadvertent access, or disasters and ensure the availability, integrity and confidentiality of information housed within the various technology infrastructure components. Significant focus must be applied to the

technology components supporting data / information as it is generally an irreplaceable item.

- XML (eXtensible Markup Language -- a subset of SGML [Standard Generalized Markup Language -- a system for organizing and tagging elements of a document] designed especially for Web documents) provides a direct method to share information, not through translation, but directly through XML definitions. An important aspect of future technology components, particularly those relating to Technology Methods, Staffing and Standards need to address /support this capability.
- Public-Private key encryption mechanisms are becoming prevalent, affording a level of security to all network transfers that historically was difficult and time consuming to create.
- Assistance from an automated Environment Management System is a necessity in large, diversified and geographically distributed environments such as the BLM in order to maintain accurate technology inventories, rapidly respond to needs for updating automated functionality through automated downloads, ensure software licensing is current, etc.
- Formal Change / Configuration management is required to achieve the CMM level 2 objective the BLM has set for itself. All technology infrastructure components regardless of geographic placement will need to adhere to change management policies in order to reach the goal.
- Specifying detailed hardware configurations cannot be effectively accomplished within the life cycle of much of the equipment installed. BLM should move to specifying functionality, or minimum configurations from an abstract standpoint, in order to avoid this issue.
- Six business oriented scenarios were developed to create smaller groupings from the 500+ technology components to develop a suggested implementation strategy to migrate from the current technology environment to one that will address the BLM user - technology interface requirements. The resulting components were grouped into “keep” and “retire” categories and “identified missing / future technology” components. The six scenarios are listed below along with the related BA implementation strategy as described in Section 3 of this report.
    - Knowledge Management / Workflow (BSA-Work Management)
    - Field Automation Enablement (Deployment to end User)
    - Legal Records (Security in Depth & BSA-BSA-Records Management)
    - FOIA / Privacy Act (Security in Depth & BSA-BSA-Records Management)
    - Optimize service delivery infrastructure and management (Deployment to end User)
    - Optimize development management for BLM custom applications (Security in Depth- Network reconfiguration portion)
- IT needs to be able to support a common GIS enterprise functionality within each State Office. To support that basic level of enterprise the technology will need to provide for quick data storage and retrieval of large volumes of data.

[Section 4.5.2]

4.5.3 Proposed Implementation Priorities and Staging for IT Components

Stage	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
	· **Infrastructure Support** Shared storage, and EM support infrastructure	· **High Security Perimeter** -	· **Standard database** supporting Distributed RDBMS (Informix) · CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. · **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	· High level network security provisions · **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") · **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data · **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology · **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	· **Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data)		· **Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and	· **Std. Development** and **test Methodology**, tools, and framework (A standard development process must be	· **Data Oriented Policies** - Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	· **Security** - User authentication, single sign-on, data access, etc. · **Tivoli Suite of Enterprise Management tools,**

Stage	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
	· **Application & Logic Middleware Server Environment - Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. · **Presentation Server Environment** - Websphere based		updated, without impacting the application code	implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)		**including software distribution, monitoring, etc.**
3	· **Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) · **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management · "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 · **Remote Desktop** Configuration · **GPS** capable computing device · Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	· Radio - WAN data **bridge** · **ISP** or **dial in support** - Remote Access Network Connectivity · Remote Authentication	· NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) · NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent · **Workflow** Support Sequential order of completion of various work tasks · **Public Data** (Base) **Search** Capability		· **Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices · **Remote Trusted User Support Policy** · **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls · **Remote Public User Support Policy**	· **Remote Authenticated Access** Dial in or ISP login support · **Encryption** (automatic and transparent) Data Encryption support · **Security** Considerations for **remote users** · **Smart Card / Biometric** Authentication

Stage	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
4	· **Test Workgroup Environment** - Mirror of Production Environment Capabilities · **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	· **Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support · **Open Public Access** · **Transient Tethered access** capability Support for temporary users		· **Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. · **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	· **Document Management Policy** Create an approach to document management and dissemination · **Reusable Skill Set** Support - Skills Availability Tracking/Sharing · **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Proposed Technology Staging

Detailed Data Recommendations (Included in Stage 1)

The following recommendations resulted from detailed technical analysis [referenced in 4.3.2]. These are intended for use in more detailed examination of software and hardware system designs.

< The BLM should develop standards to be required during application design that will define the conditions under which non-standard relational structures will be an option; the standards should require such activities to be delayed and not employed until actual demonstration of unqualified physical performance conditions.

< The BLM should establish architectural standards to be imposed upon application developers that require the use of strict metrics of critical transaction times before non-relational architectural elements can be used.

< The BLM should establish strict documentation rules for archiving design decisions that result in non-standardized data structures.

< The BLM should adopt development standards requiring the careful consideration of the overhead associated with the use of redundant physical indexes as a means of attempting performance improvements.

< The BLM should establish development and architectural standards for maintaining the integrity of derived or redundant columns in applications.

< The BLM should require developers to insure integrity between the source data and the derived or redundant data where redundant columns are imposed upon the data architecture.

< The BLM should establish a mechanism that must qualify each case where developers are allowed to add redundant columns to the architecture so as to quantify the cost/benefits in performance that is predicted from such non-relational structures.

< The MERGED data architectures should be completely specified in a resident data repository, such as the ERwin CASE suite prior to migrating the architecture to the centralized Corporate Data Repository.

< The BLM should qualify each of the current architectures if such qualification has not been done already.

< The MERGED data architecture should be reengineered to include the NIRMC/BLM proposed data element CLASSWORD standards.

- The BLM should consider the complete set of options available for managing referential integrity as shown in the BA model analysis backup volumes.

- The BLM should consider placing a moratorium on further development of data architectures that are still in the design stage until the above architectural standards can be applied to such data architectures.

RECOMMENDATIONS FROM BACKUP VOLUMES

PROCESS VOLUME RECOMMENDATIONS

Current

1. Complete development of the current business process model to the atomic level (level at which a process can no longer be decomposed) and has no more than one output.

2. Reengineer the current business model to compliance with the criteria used for analysis for the models created for this study. The purpose of taking this and the succeeding steps is to produce a "good" current business process model.

3. Rearrange all processes hierarchically. To do this, assemble all similar processes into separate groups and give the groups logical names that reflect the assembled processes. Assemble these groups on the similarity of the object of the action, not on the action. In other words, group them based on the noun in the process name, not on the verb. For example, assemble processes like plan for data collection, collect data, enter data, process data, etc., together in a single group. Once the hierarchy has been rearranged, eliminate all redundant processes. Then a model will exist that indicates "what" BLM currently does.

4. Perform a comparative analysis of the completed process model created from the ABC documentation with the process model contained in the 990 Enterprise Data Model. Take whatever action is necessary to complete an accurate model of all manual and automated processes within the current enterprise to the atomic level.

5. Perform a comparative analysis of the completed current process model with the current enterprise data architecture. The purpose of this analysis is to ensure that all data requirements for all processes have been identified; and that there are no processes that do not use data or data that is not used by some process.

6.Conduct a comparative analysis between the current process model and the target process model to ensure that all processes that should exist in the target environment are included in the target model.

Future

The following list presents recommendations for actions to achieve the future business process state objectives:

1. Refine the future business model (Levels 1-3) to compliance with the criteria used for analysis of both the current and future environment models. As the Level One through three diagrams serve as the basis for more detailed models, it is critical that the established models for the future environment be valid and rigorous. The Core Team met to balance and integrate the nine process models developed by subject matter experts. In their review, several questions were raised regarding the integrity of the future environment models. In some instances the future environment process models revealed duplication of processes and multiple processes containing loops.

2. Complete process modeling to Level Five or Six of detail, as required to reveal details of process steps and information requirements. Refinement can occur as part of continuing assessment of new initiatives or project proposals. Exposing the details of the future environment at these lower levels of detail will allow the BA developers to understand not only the entities involved in the architecture and the inter-relationships between them but the data elements linked to each of the entities.

3. Place the refined and more detailed process model (future state Levels 1-6) under a strict configuration management methodology and authority. Configuration management has several roles in change management. The necessity for strict adherence to a configuration management methodology ensures that changes occurring within a process and more specifically, during the development of that process, are implemented with consistency. Implementation of strong configuration management procedures is critical to support optimal design, development and cross-project integration. The primary objectives are to ensure the management of changes that impact project costs, schedules, and the effective delivery of IT services and data to business users and the ensure the cohesion of items, issues and changes that have impact across the development projects and program areas. Having a well-implemented configuration management methodology provides a mechanism to control changes and prioritize changes to best meet the business need and mitigate risks.

4. Assign BLM ownership and maintenance of all business processes, so that control and accountability for business process reengineering and automation is assigned to a particular person. Designating a single process owner as the central proponent for the reengineering and automation of the Bureau's BA ensures that there is a single responsible authority for the integration, coordination, and process standardization. Establishing ownership and accountability is essential to bringing about meaningful change. For this reason, it is particularly important to ensure that such ownership is not ambiguous, for example, shared between program and state administrations or other organizational components.

5. Implement business process change management. Change management promotes the smooth, systematic transition from the current to the future desired environment. The aim is to more effectively implement new methods and systems in an ongoing organization. The change management system must be flexible enough to foster desirable change, yet sufficiently strict to prevent unauthorized changes not approved by the business process owner and BLM management.

6. Identify and document business rules that support business processes within a software tool that will make it feasible to maintain and access these rules. Business rules prescribe how a process can use data. An example of a business rule is, "A LEASE must have an EXPIRATION DATE which occurs after the ISSUE DATE." Business rules are primarily derived from the laws, regulations, policies, and procedures that control the processes. Business rules are the link between the Process and Data components of the architecture. Therefore, to ensure consistency, the business rules must be maintained in a repository that also houses the process models and the data models. Documentation of business rules should allow for tractability by including the source of the business rule, and both the "effective" and "revoked" date of each business rule. This simplifies the maintenance of business rules as BLM guidance changes over time. This study identified previous BLM documentation of business rules; however, the rules are not in a practical repository to promote widespread reuse. BLM should consider accomplishing business rule documentation as part of developing new initiatives and projects in high-priority business areas.

7. Concentrate initial business process reengineering work on processes that rely heavily upon data management. Improvements made to data collection, storage, and access will have a positive, cascading effect upon all other processes. Initiatives to improve any of the 26 Level Three processes that focus on data collection, analysis, and compilation should account for the requirements of the other processes. In some cases, the requirements across these processes will be greatly different and should not logically be implemented collectively; however, BLM should not misconstrue processes that collect different types of data as unique processes; similar processes that deal with different data can and should be improved concurrently. Specific recommendations on the Data component of the architecture can be found in Section 4.2.2; implementation of those recommendations will support achievement of this recommendation.

8. Implement business process reengineering analysis for processes 4.0 Authorize Use and 8.0 Manage Work. These processes, as key drivers, will reap the greatest and most immediate benefits from a consolidated and streamlined approach toward the BLM's future state.

9. In all business process reengineering activities, include a fully-integrated analysis of the role of geospatial visualization and analysis in the identification of specific steps and information flows, and ensure that GIS is implemented wherever, objectively considered, such geospatial representation will streamline, consolidate, and improve the cost-effectiveness of performing each business process. Cease to consider GIS as an exotic technology, and start to incorporate it into the detailed workings of each business process.

DATA VOLUME RECOMMENDATIONS

The following Data Recommendations for BLM come from the notebook titled Business Driven Data Architecture. They can be located in the "Current" section, in a sub-document titled "Data Findings and Recommendations: Summary: Merged BLM Current Enterprise Data Architecture." The first group of recommendations are from Chapter 3 of that document.

Chapter 3- Recommendations for Future Data Management

Recommendation #1: Relating to the Management of Entity Types and their Primary Keys

It is recommended the BLM develop standards to be required during application architecting that will define the conditions under which reengineering/denormalization will be an architectural option; such standards should require the reengineering/denormalization activities to be delayed and not employed until actual demonstration of physical performance conditions that are within the BLM's performance standards.

Since the SQL DDL file used during the reverse engineering process was provided prior to the physical deployment of the MERGED DBMS, it is assumed that any decisions to reengineer/denormalize the MERGED relational structures was either 1) the result of adequate test cases used to develop metrics relative to the access performance histories of critical transaction blocks[1], or, 2) resulted from the implementation of BLM rules for affecting reengineered/denormalized data structures; it is recommended the BLM establish strict policy statements to manage the normalization/denormalization procedures during development that govern the conditions under which 1) an application must be fully normalized prior to any denormalization; 2) an application may avoid normalization and non-relational structures may be architected during the design stage of development; 3) an application's critical transaction blocks must be identified as candidates for denormalization prior to actual denormalization of the structures; and, 4) metrics and test cases must be defined and applied to an application's critical transaction candidate(s) to measure actual performance.

Denormalization is a handy crutch, always available to software architects, and its abuse is extraordinary. *The BLM is urged to develop architectural standards to prevent this potential design abuse.*

Recommendation #2: Relating to the Management of Entity Types and their Logical Foreign Identifiers

[1] Critical Transactions would be those considered, during the design stage, as unlikely to mjeet performance requirements, or, had proven to not satisfy performance requirements during testing or during actual production activities..

It is recommended the BLM develop standards to be required during application architecting that will define the conditions under which the modality and normalization of independent PIs will be allowed to be architected as independent ETs with “SET NULL” existence; such standards should require disciplined and exacting architectural standards under which these conditions will be employed in designing an application’s data structures.

Denormalization and its concomitant, “SET NULL” referential integrity options, are conveniently expedient approaches to avoiding assumed performance issues in the deployed application and are always available to software architects. The abuse of these expedient approaches is extraordinary; t*he BLM is urged to develop architectural standards to prevent this potential design abuse; their use should be avoided until actual performance test data dictates these compromising approaches to data architecture.*

Recommendation #3: Relating to the Management of Parent to Child Business Rules

It is recommended that the BLM use the table of Parent to Child MERGED Business Rules to qualify each of the architectural constructs in the current data model if such qualification has not been affected already.

It is recommended that the BLM establish architectural standards for data architectures that will be imposed upon all new application development and on all reengineering efforts; these standards should include the conditions under which PIs, FIs, modalities, cardinalities, referential integrity constructs, and denormalization will be allowed to be altered to accommodate architectural options and compromises in their data architectures.

It is critical that BLM development managers assure that these architectural design habits do not negate the enormous benefits to be derive from the “Two-Phase Commit” technology resident in the native DBMS system used by the MERGED application.

The above tables suggest the BLM is failing to use an enormous technical resource in the INFORMIX DBMS when it comes to managing business constraints to establish and maintain an application’s data integrity in the context of Parent/Child existences is concerned.

Recommendation #4: Relating to the Use of Child to Parent Business Rules

The reader is referred to additional Evaluation and Findings and concomitant Summary and Recommendations in relation to parent/child business rules; these additional data can be found above.

Recommendation #5: Relating to the Use of NIRMC CLASSWORDs Naming Standards

It is recommended that the MERGED data architecture be reengineered to include the

NIRMC/BLM/DA proposed data element CLASSWORD standards.

Recommendation #6: Relating to the Use of Redundant Physical Indexes

It is recommended the BLM establish architectural standards to be imposed upon application developers that require the use of strict metrics of critical transaction times before denormalization can be used to implement redundant, or surrogate, PIs or Fis.

It is also recommended the BLM establish strict documentation rules for archiving the reengineering of normalized structures into denormalize and redundant key structures.

It is recommended the BLM development standards the careful consideration of the overhead associated with use of this approach to denormalizing critical key structures.

Recommendation #7: Relating to the Use of Inconsistent Data Types in Foreign Keys

It is recommended that the BLM consider the reengineering of these MERGED physical structures so as to eliminate these occurrences of inconsistent physical data types between the Primary Keys and their Foreign Keys so as to make the independent and dependent data types the same in all occurrences.

Recommendation #8: Relating to the Use of Redundant Columns

It is recommended the BLM establish development and architectural standards for maintaining the integrity of such occurrences of derived or redundant columns in applications such as MERGED; if performance problems are anticipated with critical SQL statements that join to retrieve columns for the purpose of filtering, then the tables used by the join operation may be candidates for denormalization (note that these are candidates only, to begin with).

Attempts can be made to identify such situations during the physical design of application architectures such as MERGED by conducting performance testing on the tables and functions in question; it is advised, strongly, that the BLM developers avoid guessing about performance issues and to use test results only to guide reengineering/denormalization activities;

It is critical that application developers remember that derived or redundant structures and their stored data must be maintained; that is, the BLM must insure integrity between the source data and the derived or redundant data (in this case, it is assumed the transmittal ET is the original source data since it is the independent ET where counts of currency are transmitted to the MERGED application).

It is critical for application developers to consider the volatility of the source column(s) and rows when deciding to use derived or redundant data structures; if the source information is constantly

being updated, the application may incur severe performance penalties in maintaining integrity between the primary data and copies of that data.

The BLM is advised that adding redundant columns to the data architecture means deliberately adding overhead to maintain these replicated columns; a decision must be made in each case whether the gain in performance is worth the cost in overhead.

If the redundant column(s) is fairly volatile (subject to frequent modification (update)), the developer should consider opting against this deliberate use of redundant columns as an architectural solution.

This evaluation was not able to determine if SQL triggers were employed in maintaining these redundant copies of the source data (this is the most common method used—a trigger fires automatically to update any data based on the source data) it is recommended the BLM developers always use triggers to maintain derived or redundant.

It is recommended the BLM not use application maintenance code to maintain data integrity in these cases; it can expose application data to integrity problems; data integrity may be seriously compromised if users are allowed to update the source data directly (using querying applications such as BRIO) , instead of using the application; furthermore, in these situations (which appear to be very abundant in the MERGED application) the MERGED application's data integrity is extremely vulnerable to a potential lack of synchronization and unintended , costly duplication of effort in maintaining the redundant data.

The BLM is urged to avoid such application-dependent columns if at all possible.

The benefits and costs of the deliberate use of redundant columns as an architectural option are listed here:

Column-level denormalization on lookup or parent tables provide the following benefits:

- Better response times or throughput through the elimination of the join;
- The chance to eliminate a foreign key, primarily if the lookup table can be collapsed;
- The reduction of lock contention that cuts down blocking or deadlock situations depending on the nature of the MERGED transaction.

Potential costs of using this design option are as follows:

- The modified table will grow in size; adding columns to the table will result in a wider row; in particular, fewer rows can be stored on a memory data page; therefore, storing the table-level information takes more memory pages;
- The larger number of data pages will slow performance queries not benefiting from the elimination of the join, as the number of I/Os required to process the table is greater;
- The duplicated column data will require maintenance, perhaps through triggers, to ensure that duplicated columns are kept up to date; this performance penalty can be sever in situations where the column to be duplicated is volatile (subject to frequent modifications);

- The design of transactional blocks in the INFORMIX DBMS will become more complicated as use is made of the “Two-Phase Commit” mechanisms resident in the DBMS (it is assumed that each occurrence of the multiple columns must be a member of any transactional recover approach engineered into the application’s recovery design.)

Recommendation #9: Relating to the Matter of Inconsistent Supporting Documentation

That, in the future, the MERGED data architecture be completely specified in the resident data repository, such as the ERwin CASE suite.

That all narrative content, i.e. definitions, descriptions, comments, be constructed in the resident repository.

That all such non-structured narrative specifications not be developed and supported in an external COTS system, such as a word processing suite.

All such non-structured specifications be built, stored, and maintained in a singular data store such as the resident ERwin CASE suite.

That the supporting non-structured specifications for all data architectures be baselined (qualified) and maintained under strict Quality and Configuration Assurance control.

Recommendation #10: Relating to the Use of Super-Type and Sub-Type Entity Type Structures

It is recommended that the BLM consider reengineering any of the candidate ATs into subtype structures since the logical representation of data structures as subtypes of super type structures is very facilitating to Subject Matter Experts and can provide more economical storage structures in their physical state.

It is recommended the BLM consider the use of Sub-typing as a means of reducing table row sizes to facilitate performance during update/retrieval executions; a single supertype table, which contains columns in common, and multiple subtype tables containing differentiating columns may be more efficient than a single supertype table containing all columns.

Recommendation #11: Relating to the Use of Business Subject Areas

BLM SMEs should consider if any of the ETs are subject to allocation to more than one Subject Areas, which is quite often the case in Subject Area partitioning; where such instances occur, the cardinality of these relationships must change from 1:M to M:M to effect integrity in the representation.

The single most important structural property between two data structures is the cardinality

existing between the two structures; as such, the potential M:M cardinality between ETs and ATs must be carefully architected when generating business data subject areas as part of the application's data architecture.

It is recommended the proposed NIRMC data administration standards include Subject Area constructs.

Recommendation #12: Relating to the Use of Referential Integrity Technologies

It is recommended that in the future the BLM consider reengineering the entire MERGED architecture to affect consistent design intent in the context of maintaining referential integrity of values in the MERGED production environment. The technological resources are available, already, within the INFORMIX DBMS currently employed by the BLM.

The maintenance of good data integrity will result in enormous economies to the BLM in future use of this important area of business.

It is recommended the BLM consider the complete set of options available for managing referential integrity; these recommended options include the conditions and rules in the following table:

	Identifying Relationship	**Non-Identifying Relationship (Nulls Allowed)**	**Non-Identifying Relationship (No Nulls)**	**Subtype Relationship**
Parent Insert Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Parent Insert Trigger Default	NONE	NONE	NONE	NONE
Parent Update Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Parent Update Trigger Default	RESTRICT	SET NULL	RESTRICT	CASCADE
Parent Delete Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Parent Delete Trigger Default	RESTRICT	SET NULL	RESTRICT	CASCADE
Child Insert Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Child Insert Trigger Default	RESTRICT	SET NULL	RESTRICT	RESTRICT
Child Update Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Child Update Trigger Default	RESTRICT	SET NULL	RESTRICT	RESTRICT
Child Delete Trigger Choices	RESTRICT, CASCADE, NONE	RESTRICT, CASCADE, SET NULL, SET DEFAULT, NONE	RESTRICT, CASCADE, SET DEFAULT, NONE	RESTRICT, CASCADE, NONE
Child Delete Trigger Default	NONE	NONE	NONE	NONE

Recommendation #13: Relating to the Proposed Data Administration Standards

It is recommended the Data Administration manual be modified to include a proactive administration of requisite data standards to prevent the instantiation of unqualified data that must be qualified at enormous cost.

It is recommended the BLM empower the Data Administration unit to establish all standards relating to data architecture; to implement such architectural standards upon application development; and that this administrative unit be empowered to enforce such architectural standards upon all BLM data assets.

It is recommended the BLM immediately engage in a re-culturalization of its Data Administration resources to migrate the staff from a role of metadata archivists to a dynamic role of architectural engineers with the richest source of data engineers in the Bureau.

The following Data recommendations are located in the same sub-document titled "Data Findings and Recommendations: Summary: Merged BLM Current Enterprise Data Architecture."
They are extracted from the tables found in Chapter 4, Section 4.1. These tables also contain Architectural Issues, Category of Activity and a Priority ranking. They are listed here using the "Merged Unique Priority Ranking". A second table is located in the document that lists the recommendations ranked first by "Category of Activity" and where there were conflicts, the "Merged Unique Priority Ranking" was used to sort further.

This listing may appear to duplicate some recommendations and should be viewed in the context of the document it came from.

Recommendations:

It is recommended the Data Administration manual be modified to include a proactive administration of requisite data standards to prevent the instantiation of unqualified data that must be qualified at enormous cost.

It is recommended the BLM empower the Data Administration unit to establish all standards relating to data architecture; to implement such architectural standards upon application development; and that this administrative unit be empowered to enforce such architectural standards upon all BLM data assets.

It is recommended the BLM immediately engage in a re-culturalization of its Data Administration resources to migrate the staff from a role of metadata archivists to a dynamic role of architectural engineers with the richest source of data engineers in the Bureau.

It is recommended the BLM develop standards to be required during application architecting that will define the conditions under which denormalization will be an architectural option; such standards should require the denormalization activities to be delayed and not employed until actual demonstration of physical performance conditions that are within the BLM's performance standards.

It is recommended the BLM develop standards to be required during application architecting that will define the conditions under which the modality and normalization of independent PIs will be allowed to be architected as denormalized and "SET NULL" structures. Such standards should require disciplined and exacting architectural standards under which these conditions will be employed in designing an application's data structures; denormalization and its concomitant "SET NULL" referential integrity options, are conveniently expedient approaches to avoiding assumed performance issues in the deployed application and are always available to software architects. The abuse of these expedient approaches is extraordinary.
The BLM is urged to develop architectural standards to prevent this potential design abuse. Its use should be avoided until actual performance test data dictates these compromising approaches to data architecture.

It is recommended that the BLM establish architectural standards for data architectures that will be imposed upon all new application development and on all reengineering efforts; these standards should include the conditions under which PIs, FIs, modalities, cardinalities, referential integrity constructs, and denormalization will be allowed to be altered to accommodate architectural options and compromises in their data architectures; it is critical that BLM development managers assure that these architectural design habits do not negate the enormous benefits to be derive from the "Two-Phase Commit" technology resident in the native DBMS system used by the MERGED application.

It is recommended the BLM establish architectural standards to be imposed upon application developers that require the use of strict metrics of critical transaction times before denormalization can be used to implement redundant, or surrogate, PIs or Fis.

It is recommended the BLM establish strict documentation rules for archiving the reengineering of normalized structures into denormalized and redundant key structures.

It is recommended the BLM development standards requiring the careful consideration of the overhead associated with the use of redundant physical indexes as a means of denormalizing critical key structures.

It is recommended the BLM establish development and architectural standards for maintaining the integrity of occurrences of derived or redundant columns in applications such as MERGED.

It is recommended the BLM force developers to insure integrity between the source data and the derived or redundant data where redundant columns are imposed upon the data architecture.

It is recommended the BLM develop standards that assure developers are required to consider the volatility of the source column(s) and rows when deciding to use derived or redundant data structures.

It is recommended the BLM develop software engineering standards to manage the design conditions that allow the adding of redundant columns to the data architecture since this means deliberate addition of overhead to maintain these replicated columns.

It is recommended the BLM establish a data architecture assurance mechanism that must qualify each case where developers are allowed to add redundant columns to the architecture so as to quantify the cost/benefits in performance that is predicted from such non-normalized structures.

It is recommended the BLM developers always use triggers to maintain derived or redundant data structures.

It is recommended the BLM **not use** application maintenance code to maintain data integrity in cases where deliberate addition of redundant columns is allowed in applications; it can expose application data to integrity problems; data integrity may be seriously compromised if users are

allowed to update the source data directly (using querying applications such as BRIO), instead of using the application.

It is recommended the MERGED data architecture be completely specified in a resident data repository, such as the ERwin CASE suite.

It is recommended all narrative content, i.e. definitions, descriptions, comments, for the MERGED application be constructed in a resident repository.

It is recommended all non-structured narrative specifications (documentation) **not be** developed or supported in an external COTS system, such as a word processing suite.

It is recommended that supporting non-structured specifications (textual documentation) for all data architectures be baselined (qualified) and maintained under strict Quality and Configuration Assurance control.

It is recommended all non-structured specifications (documentation) be built, stored, and maintained in a singular data store such as the resident ERwin CASE suite or the BLM Repository.

It is recommended the BLM consider reengineering any of the candidate ATs in the MERGED data architecture into subtype structures since the logical representation of data structures as subtypes of super type structures is very facilitating to SMEs and can provide more economical storage structures in their physical state.

It is recommended BLM SMEs consider if any of the ETs allocated to MERGED Subject Areas need to be allocated to more than one Subject Area and, in such cases, reengineer the cardinality of these structures from 1:M to M:M.

It is recommended that the BLM qualify each of the architectural constructs in the current MERGED data model if such qualification has not been affected already.

It is recommended that the MERGED data architecture be reengineered to include the NIRMC/BLM/DA proposed data element CLASSWORD standards.

It is recommended that the BLM consider the reengineering of MERGED physical structures so as to eliminate occurrences of inconsistent physical data types between the Primary Keys and their Foreign Keys so as to make the independent and dependent data types the same in all occurrences.

It is recommended the BLM consider reengineering the entire MERGED architecture to affect consistent design intent in the context of maintaining referential integrity of values in the MERGED production environment. The technological resources are available, already, within the INFORMIX DBMS currently employed by the BLM.

It is recommended the BLM development managers employ good data integrity to effect economies to the BLM.

It is recommended the BLM consider the complete set of options available for managing referential integrity; these recommended options include the conditions and rules in the table shown under section 12.3.2, above.

It is recommended the BLM consider placing a moratorium on further development of data architectures that are still in the design stage (have not been qualified (baselined)) until the above architectural standards can be applied to such data architectures.

APPLICATIONS VOLUME RECOMMENDATIONS

Target Applications Status and Observations

One Enterprise, One Interface:

All systems should use a (windowing) Graphical User Interface (GUI)
- Commercial Applications
- Custom Applications
- Operating Systems
- Communications Systems

All applications should be modular in design
- Platform independent
- Non-proprietary data formats
- Meta-Frame compliant

All applications should be Internet ready
- Full publishing capabilities
- Full subscription capabilities
- Fully secure transmissions

All applications should conform to enterprise wide applications modeling
- The quality of application development has been commented on in a separate summary regarding engineering, documentation and scripting. (SOZA DC)

Deployment:

BLM IT factory hosting enterprise applications and data at all major locations
BLM trusted users operating through an intranet
BLM public users operating through the Internet

Virtual GIS server farm using a single interface
- Distributed non-editable GIS files
- Centralized (virtual) editable GIS files

Defined and scripted Intranet/Internet Push/Pull automation
E-Commerce transaction integration to support workflow

Management:

Mission Critical applications should be common to all the BLM
Mission Essential applications should be common to all the BLM

Tier Three applications should be divisional domain systems

A single clearinghouse for application design QA and LOS

Recommendations Specific to GIS

Applications need to be selected or developed that will allow the distribution of geospatial information and tools to the end user.

The current Beta Testing process within BLM for GIS software (ESRI Products) is in need of review and update.

There should be more coordination of GIS efforts above the State Office Level.

Review of RDMS used for GIS and corporate. The future of GIS has all data more closely associated with commercial RDBMS systems.

The BLM should bring its GIS to a somewhat consistent level throughout the Bureau and start using Spatial Database Engine (SDE) before trying to complete a bureau-wide implementation Arc/Info version 8. Trying to do both at the same time would be too much. The implementation of an "Enterprise GIS" should proceed using small obtainable goals that can be managed within constraints of the BLM's business.

TECHNOLOGY

Additional detail regarding the six technology scenarios summarized in the Summary Report are presented in the following pages.

Scenario: Optimize the service delivery infrastructure and management
How to implement a logical architecture for the hardware, software and infrastructure to provide effective BLM operations

Business Problem:

- Autonomous State operations preclude potential synergies
- BLM infrastructure, data, and application architecture presents difficulties in achieving data consolidation, cross-boundary reporting, etc.
- Current environment difficult to manage, and does not lend itself to offering increased levels of service delivery.

Technology Overview:

- Each state has a separate data model, server environment, application, etc in other words, a unique business environment. However, every state is under the same Federal regulations, and, except for the state specific attributes, have a common function to perform.
- Optimize the I/T environment to facilitate the service delivery business of the BLM, not impede it!

Recommendations:

- Create a standard data model, common among all state applications
- Create a multi-level infrastructure that facilitates performance, while minimizing management effort.
- Centralized infrastructure increases performance and capabilities (e.g. centralized reporting) while reducing management

Optimize IT Service Delivery and Management

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment - Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX** (Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Scenario: Field Automation Enablement

- How to exploit technology to enhance the capabilities – and capacities - of the field staff

Business Problem:

- Field operatives have little or no automation in place to assist them in their job function.

Technology Overview:

- Handheld computing and remote communications have made great strides in recent years – or months. The new HandSpring Visor uses the Palm OS, and has a large memory capacity as well as an expansion slot, affording remote communications capabilities and GPS.

Recommendations:

- Perform a user needs analysis on the field community to determine how automation, communications, and connectivity with electronic sources can improve their ability to perform and enhance their work environment.

Field Automation Enablement

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Scenario: Knowledge Management/Workflow

- How to mitigate the "brain drain" of retiring work force, and consistently perform service delivery decisions using available data, as well as publicize I/T capabilities available to enhance the employee environment

Business Problem:

– NIRMC has some 40% of the employee staff within 5 years of retirement. The BLM overall, is not much different demographics

– Field staff retains much of the knowledge as to how to process their work, totally undocumented

– BLM has become entangled in litigation over BLM field operatives' inconsistent decisions, using identical source data

– NIRMC does not have a good reputation within the user community, yet offers capabilities that enhance the work environment.

– I/T Enterprise Service capabilities currently in place have been underutilized, leaving the BLM with "stovepipe" systems, and significant effort required to optimize the resultant systems. (e.g. CDD is in place, but not used, potentially due to developer ignorance of the availability of such development aids.)

Technology Overview:

– BLM has ubiquitously deployed the premier knowledge management and workflow tool on the market, albeit currently only using the Email portion of the product

Recommendations:

– Create NOTES knowledge bases for process descriptions, "pushing" the content to the employee community. Additionally, leverage the web interfaces to NOTES to publish information that can be "pulled" through ubiquitous web browsers.

– Create NOTES workflow processing environments, leveraging the NOTES infrastructure as well as the knowledge bases of BLM processes.

Knowledge Management/Workflow

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Scenario: Optimize Development Management for BLM Custom Applications

- How to manage the development activity, both in-house and contractors

Business Problem:

- Applications are developed along SEI CMM Level 1 approaches – Ad hoc development – where non repeatable processes and approaches are used. The only possibility of success in application development in this mode is with high performance talent.
- Data dictionaries and other code repositories are not established or enforced, therefore synergies between applications is non-existent.
- CASE (Computer Aided Software Engineering) is not uniformly applied.
- No consistent software development methodology is in place, therefore no predictable completion estimate can be made as it would have no basis in historical fact or precedent.

Technology Overview:

- Software tools and standardized process approaches have proven to significantly improve quality while decreasing time to market.

Recommendations:

- Establish code, data dictionary, and rules repositories, and enforce their use on all new application development activity.
- Establish metrics measurement for compliance against Software Engineering Institute Capability Maturity Model, with the goal of attaining Level 3 in 2 years.
- Establish a standard tool set and tools, methods, and approaches to software development practices.

Optimize Development Management for BLM Custom Applications

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Scenario: Legal Records

- How to move to electronic legal records

Business Problem:

- BLM records are currently hard copy, creating performance and logistical problems in retrieval.
- Electronic representations are either facsimiles of the hardcopy or in-process transaction data
- Production transaction server data is portrayed as a valid representation of legal records. This data is, by default, used as legal records. Only in a dispute, does the actual hard copy record become part of the effort.
- There is no review process for entered data to be validated prior to committing it to electronic medium.
- Production data servers are simultaneously used for records retrieval, without validation.

Technology Overview:

- Random access storage and retrieval satisfied the technology characteristics required, albeit low performance needs (non-transaction based system).
- Physical and electronic security considerations would need to be incorporated.
- Workflow would have to be modified to incorporate a commit process to establish legal records validity.

Recommendations:

- Create a Master Legal Records Server
- Create a commit process to populate a commit cache of validated records
- Provide for secure updating the Master Legal Records Server

Provide electronic legal BLM Land & Minerals records

- Provide a secure storage environment
    - No direct user access – no transparency to this resource
        - Legal records server will request data update (pull, not push)
    - No non-verified updates
        - Establish commit process for transaction data to become legal
            Verified data prior to committing it to legal records status
    - Maximum security currently available
        - Behind high security Security Perimeter
        - Off-site storage
        - Use separate protocol (not supported by BLM as a whole)
        - Use a random port
        - No published router tables
        - Any console within physical and logical security perimeter
        - Perimeter proxy for server
        - No external knowledge of NIC/MAC

Legal Records

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	

Scenario: FOIA/Privacy Act

Business Problem:

- Ensure that Public Data, not protected by the Privacy Act or National Security Interested, be available for public access
- Eliminate significant security risks (open access), or flexibility limitations (public rooms) that exist in the Current IT Architecture.
- Minimize Effort Required for Network and Security Management
- Provide Trusted Electronic Data Access to All Trusted Users
- Prevent Trusted Access for Untrusted Users – Minimize Exceptions to Security Policy

Technology Overview:

- The current public access approach, public rooms, technically satisfies the need, but is not the most effective way to disseminate information to a large user population.
- Security of network infrastructure would have to be designed to facilitate this effort.
- "Defense in Depth" provides manageable layers of interaction

Proposed Solution Space:

- BLM, USDA (FS), USGS, MMS, etc. should all be "trusted" users; Public should be treated as "untrusted" but with read-only access to relevant published data.
- Create a layered network/security infrastructure that facilitates the varying security requirements of replicate or distribute region specific data, as appropriate.

FOIA/Privacy Act

Sequence	Computing Platforms	Data Communications	Data Mgmt & Structure	Development Tools	Methods, Staffing & Stds.	Enterprise Mgmt & Security
1	**Infrastructure Support** Shared storage, and EM support infrastructure	**High Security Perimeter** -	**Standard database** supporting Distributed RDBMS (Informix) CA Platinum **Data Repository** - Oracle Shared data repository for Corporate Data Dictionary, data models, etc. **Info Dissemination** - Related to knowledge management, a repository of varied and diverse topics needs to be on-line and searchable by anyone in BLM. Items such as Information Management Bulletins, etc. Provides a dynamic capabilities marketing vehicle to enhance employee performance.		Vendor/Contractor Management	**High level network security provisions** **Security Perimeter Level 1** Environment - (no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a secure back end environment, supporting the legal records "data warehouse") **Security Perimeter Level 2** Environment. - A "DMZ" style data security perimeter. Behind this Perimeter would be the R/W servers - the "data marts". Direct R/W access allowed for authorized users, R/O access for all to published data **Security Perimeter Level 3** desktop access - All service delivery desktops would be protected by biometric or smart card technology **Security Perimeter Level 4** Remote public access - All service delivery published data would be accessible through public commodity interfaces.
2	**Data Server Environment – UNIX (**Security Perimeter Level 2 Environment - direct R/W access allowed for authorized users, R/O access for all to published data) **Application & Logic Middleware Server Environment Mixed Platform as appropriate** NT Primary, UNIX as appropriate. From this layer down, outside security perimeters, and relies on OS security. **Presentation Server Environment** - Websphere based		**Business Rule Abstraction** Database development discipline that requires that logic be segregated from the code, so that the business logic can be consistently be reused and updated, without impacting the application code	**Std. Development** and **test Methodology**, tools, and framework (A standard development process must be implemented, so engineering discipline can be incorporated into the IT development efforts. Evolutionary approaches, with small, incremental product releases, should be used.)	**Data Oriented Policies -** Data Retention Policy Data Archive Policy Data Storage Policies, Data Backup/Restore Policies	**Security -** User authentication, single sign-on, data access, etc. **Tivoli Suite of Enterprise Management tools, including software distribution, monitoring, etc.**
3	**Legal Records Repository Environment – UNIX (**Security Perimeter Level 1 Environment - no end user direct access allowed, updated on a pull basis from data server environment. Effectively, a data warehouse) **Workgroup Computing** Notes Email, OA services, Document Management, Knowledge Management "Proxy" environment of Level 2 Servers, minimizing the "holes" to manage into Level 2 **Remote Desktop** Configuration **GPS** capable computing device Commodity **Handheld Computing Device** w/proprietary enhancements Handspring Visor, Palm Pilot or Windows CE devices-	**Radio - WAN** data **bridge** **ISP** or **dial in support** - Remote Access Network Connectivity Remote Authentication	NOTES **Knowledge** and **workflow management** forums -(Leveraging NOTES, provide the ability to knowledge base repositories to be set up, maintained, and disseminated. Capturing and publishing the human knowledge factor is probably the most important thing that IT can facilitate within the BLM environment.) NOTES/Domino **Document Management** - Currently Email is the dominant tool of document management. Revision control is non-existent **Workflow** Support Sequential order of completion of various work tasks **Public Data** (Base) **Search** Capability		**Handheld Device Interface Policy** Create an approach to handle portable and handheld computing devices **Remote Trusted User Support Policy** **Credit Card Support** Policy consistently handle credit card transactions on-line w/appropriate fiduciary controls **Remote Public User Support Policy**	**Remote Authenticated Access** Dial in or ISP login support **Encryption** (automatic and transparent) Data Encryption support **Security** Considerations for **remote users** **Smart Card / Biometric** Authentication
4	**Test Workgroup Environment** - Mirror of Production Environment Capabilities **WinTerm/NetPC Windows** Terminals provide an easier environment to manage with limited staffing resources and broad geographical dispersion (roving desktop and application support)	**Credit Card** Clearinghouse Access Credit Card processing support, for on-line transaction support **Open Public Access** **Transient Tethered access** capability Support for temporary users		**Development and Test Environment** - A standard test environment, distinct and separate of the production environment, needs to be established, with associated resources and tools. **Development tools** in support of n-Level, web-enabled application delivery JAVA - servlets, applets, and applications. As a stand-alone environment, JAVA offers synergistic development with web-based approaches.	**Document Management Policy** Create an approach to document management and dissemination **Reusable Skill Set** Support - Skills Availability Tracking/Sharing **Programming Skills** SQL, 4th generation language programmers, for database environments, plus test capabilities	