




Washington State Administrative Office of the Courts

Superior Court Management Feasibility Study

**Technical Requirements
Version 4.4**

Deliverable 4

PSC 11062 Superior Court Management Feasibility Study Project

Authored by:	Mr. Robert Marlatt
Telephone:	206-442-5010
E-Mail:	rmarlatt@mtgmc.com
Date:	March 2, 2011

TABLE OF CONTENTS

I.	Introduction	4
	A. Purpose.....	4
	B. Assumptions.....	4
II.	Technical Requirements.....	5
	A. Application Requirements.....	5
	B. Information Requirements	11
	C. Infrastructure Requirements.....	12
	D. Security Requirements.....	15
III.	Data Dependencies	17
IV.	Document Approval.....	21

Document History

Author	Version	Date	Comments
Robert Marlatt	1.0	11/24/2010	Initial draft.
Robert Marlatt	2.0	11/29/2010	Added service requirements. Several corrections.
Robert Marlatt	3.0	12/6/2010	Changes based upon Superior Court Management Feasibility Study (SCMFS) team comments. Placed in correct document format.
Robert Marlatt	3.1	12/6/2010	Changes based on Eric Kruger feedback.
Robert Marlatt	3.2	12/10/2010	Respond to feedback. Added endnotes.
Robert Marlatt	3.3	12/15/2010	Combined documents (Eric Kruger comments).
Robert Marlatt	4.0	12/17/2010	Combined categories and made edits according to team work session held December 16, 2010.
Robert Marlatt	4.1	1/5/2011	Incorporated edits and upgraded many requirements. Added data dependencies section.
Robert Marlatt	4.2	1/25/2011	Edits from Eric and Sriram. Added picture to data dependency chapter.
Robert Marlatt	4.3	2/24/2011	Kate Kruller proposed several standards to be included in the technical requirements.
Robert Marlatt	4.4	3/1/2011	Review by and edits from Gary Guinotte, AOC Solutions Architect.

I. Introduction

This section provides the purpose and context for the technical requirements document.

A. Purpose

The purpose of this document is to provide technical requirements, necessary to support court case management and calendaring functions and other business functions of the Superior Courts. It also identifies the data dependencies between a future provider solution and the existing Judicial Information Systems (JIS).

The technical requirements consist of the application, information, infrastructure, and security requirements that support the business functions of the courts case management and calendaring function. Another document, Deliverable 3 – Business Requirements, defines the functional and behavior requirements for the superior court case management and calendaring system.

MTG Management Consultants, LLC, proposed service requirements that consist of systems integration and support and maintenance requirements. These requirements are in a separate document. MTG plans to incorporate these service requirements in the procurement Request for Proposal (RFP) (Deliverable 11) statement of work.

The Administrative Office of the Courts (AOC) project team developed an initial draft of non-functional requirements. These requirements were transformed into a categorization scheme similar to that for the AOC enterprise architecture. This approach ensures that requirements are elicited for each architecture category.

B. Assumptions

- These requirements will need to be reviewed and adapted based upon the results of the feasibility study.
- The application will be implemented within the enterprise architecture; information networking hub capabilities will be operational prior to the purchase of a vendor solution.

II. Technical Requirements

This section describes the technical requirements for the Superior Court case management and calendaring system.

The technical requirements are organized into the following groups:

- Application.
- Information.
- Infrastructure.
- Security.

A. Application Requirements

Application requirements describe the required capabilities and attributes that AOC expects from a commercial application. These requirements include the capabilities and processes for managing the application components and structures.

The application requirements are organized in the following categories:

- Access Layer.
- Application (General).
- Application Development Environment.
- Documentation – Application.
- Message Broker.
- Usability.

ID	Type	Requirement	Source
Access Layer			
1	M	The provider solution shall be compatible with all AOC-supported versions of Internet Explorer (IE).	2.06
2	M	The solution shall allow access from multiple venues, including from a secured site on the Web.	1.03
3	HD	The solution should follow Mobile Web Best Practices (MWBP). [www.w3.org/TR/mobile-bp]	23.01.01 23.01.02 23.01.03
4	HD	The solution should be capable of providing remote access (i.e., access to the application outside of court offices).	21.07
5	D	The solution should be compliant with Web 3.0 standards.	2.07
6	HD	User interface (UI) changes should be made by means of a cascading style sheet or other method that allows changes to the UI to be applied globally to all screens.	10.05
7	HD	The solution should follow the Web Content Accessibility Guidelines (WCAG) 2.0. [www.w3.org/TR/WCAG20].	1.02
8	HD	The system should provide Inquiry users with the ability to have limited or "read-only" access to specified portions of the systems.	MTG

ID	Type	Requirement	Source
9	HD	All applications provided to AOC are to follow the Microsoft Windows User Experience Guidelines ¹ and provide a consistent, branded interface across all UI devices (i.e., Back Office, Web).	MTG
Application (General)			
10	M	Special modifications to COTS ² package software code that create a special version for the AOC shall not be allowed.	10.02
11	M	The solution shall be modularized and organized in an n-tier architecture.	2.01
12	M	The solution shall maintain a record of all configuration changes.	3.02
13	M	The solution shall provide logging capabilities that are configurable.	21.06
14	M	New versions of the application shall be backward compatible with older supported versions.	11.10
15	HD	The solution provider may propose a hybrid application. AOC prefers that this type of hybrid application solution: <ul style="list-style-type: none"> • Operate on a single code base for the state. • Be highly configurable. • Support local court processes and local configuration. • Minimize customization of underlying software code. • Provide a method for tracking all changes from the vendors' primary and current code base. The solution provider must disclose all points of customization to accommodate the AOC business functionality.	MTG
16	HD	The solution should be able to adopt and extend service-oriented architecture (SOA) framework as the service delivery mechanism.	13.05
17	HD	Any enhancement/change to the application should work as an integrated feature of the overall application.	11.04
18	HD	The application should allow optional features to be added and removed on demand without affecting the overall application functionality or performance.	11.05
19	HD	The solution should provide remote access (i.e., the ability for local courts to configure their use of the application) for user account management and application configuration.	14.02
20	HD	The solution should have a separate monitoring console UI showing various stages and states of the application with intuitive color-coded message to indicate the solution state at any given time.	12.10

¹ See www.microsoft.com/downloads/details.aspx?FamilyID=B996E1E7-A83A-4CAE-936B-2A9D94B11BC5&displaylang=en.

² "COTS" is defined as: "Item that is commercially available, leased, licensed, or sold to the general public and which requires no special modification or maintenance over its life cycle." Examples of COTS packages include Microsoft Office products, Microsoft Exchange, or Intuit Quicken. The vendors do not customize or adapt these products to individual customer context or needs.

ID	Type	Requirement	Source
21	HD	The solution should allow for auto-monitoring with no human intervention. The system should have the ability to monitor various aspects of the system operations, collect and report metrics, and initiate notification actions when the system is out of established tolerance levels.	12.07
22	H	The solution should initiate standard responses when a business event is recognized. The solution should be capable of initiating a notification (e.g., e-mail), initiating a work flow process, or taking steps to perform a predefined functionality in response to an event.	MTG
23	HD	Changes to edits and business rules should be made through configuration parameters and properties. Data items should be modifiable through local object properties. Programmatic validation edits should be configurable. Business rules should be configurable by a court subject matter expert (SME).	10.04
24	HD	The application should be nimble enough to adapt to new changes in the business rules as well as hardware changes.	11.03
25	HD	Business rules should be externalized from the application and should be accessible through standard application program interfaces (APIs) independent of the solution.	2.10
26	HD	The solution should allow application jobs (examples: reports, extracts, data loads) to be scheduled for unattended operation.	14.05
27	HD	The interface should allow operations to be executed in batch form (example: modify the attributes of a set of users).	14.03
28	HD	The application should use generic search capabilities to search for any information relating to a case (person, documents, court officers, related cases, etc.).	MTG
29	HD	The solution should render a unified presentation interface for the external and internal users of the application.	23.01
30	HD	The solution should accommodate the ability to make searches of historical data conditionally and on demand.	MTG
31	HD	The solution should be able to dynamically retrieve existing data from other AOC/Information Services Division (ISD) and related systems (SQL Server schema or database procedure or other documented interface supplied by AOC/ISD): <ul style="list-style-type: none"> • General person information – name, residence address. • Unique ID. • Picture. • Alias(es). • Contact information – telephone, e-mail, preferred mailing address. 	MTG
32	HD	All automatic, standard or custom reports generated by the system should format output directly in electronic and hardcopy form - such as via a printer, PDF, spreadsheet, or a user-defined e-mail address.	MTG

ID	Type	Requirement	Source
33	D	The solution should provide reporting capabilities, including pre-formatted reports within each of the dispatch subject areas as well as the ability for the system users to perform ad hoc inquiry reporting for decision support needs.	
34	HD	The solution should provide keyboard shortcuts as well as menu-based access to functions.	23.02
35	HD	The solution should provide graphical user interface (GUI) management tools to automate repetitive tasks and manage the application environment.	12.01
36	HD	The solution should allow user management tasks for a work group to be delegated to a member of that that work group.	14.04
37	HD	The application should allow journaling of all user actions for auditing purposes.	12.12
38	HD	Work flow should be controlled though a configurable work flow engine.	2.09
Application Development Environment			
39	M	Any changes made to the application (security patch, code updates, etc.) shall not break overall existing functionality(ies).	11.06
40	M	The solution shall allow interaction between applications via published interfaces rather than through direct manipulation of data.	2.08
41	M	The solution shall have APIs to the business logic layers so that data can be entered into the solution independent of a GUI.	2.02
42	M	The solution provider should provide an interface for performing remote tasks and running remote scripts.	19.10
43	M	Promoting code between two regions shall require only those two regions to be locked down for promote. All the other regions shall be available to users.	19.12
44	HD	The software written by the vendor should not be dependent upon proprietary or vendor-specific extensions to the standard libraries.	2.04
45	HD	The software should support open standards.	16.04
46	HD	All application software should be written in a common, state-of-the-art, well known, modern, high-level, and highly structured language, supportable by AOC. AOC's standards include .Net and C# under the .Net Framework or Java frameworks.	2.05
47	HD	Non-Web-based components should be compatible with one of the technologies listed below for remote control and management of equipment and software: <ul style="list-style-type: none"> • Microsoft Management Console (MMC). • Microsoft Systems Management Server. • Remote control and management. 	MTG
48	HD	All vendor-proposed software should be the current version in production at the time of beta test.	MTG

ID	Type	Requirement	Source
49	HD	All vendor-proposed software should be Year 2000 compliant in conformance with the British Standards Institute's PD2000-1 specification and ISO 8601 and ISO 8602 date specifications: <ul style="list-style-type: none"> All dates are processed using a four-digit year format. Leap years are correctly processed. 	MTG
50	HD	All vendor-proposed software should be transferable to computers running the same operating system without any modification.	MTG
51	D	Development tools and Integration tools should be available as part of the solution.	2.03
52	D	The application should allow for a version in a higher environment (typically a production library) to be brought down to the development region for code modification without having to copy that version in any of the in-between environments.	19.04
53	HD	Promoting code between environments should take less than 1 half hour for the entire task (from the time the environments are locked until the time that the environments are released for normal operation).	19.13
54	HD	The steps to promote the application from one environment to the next should be simple and easy to understand and perform with minimal training on the part of the configuration management team.	19.06
55	HD	The system should be smart enough to detect how to push out updates (in case one of the machines gets one part and another gets a second part) or tasks will need to be properly grouped together such that portions that are dependent are not split across machines.	20.04
56	HD	The application should allow for progressive promotion from one lower region to the next higher region in a predefined order.	19.02
57	HD	The application should support the coexistence of multiple versions of itself in various environments (i.e., development, test, integration, user, training, and production).	19.01
58	HD	There should be well-defined, easy-to-understand, step-by-step instructions detailing the process of moving code between environments and the shortcuts to bypass environments if need be.	19.08
59	NH	Any developer maintaining the application should be able to bring down a version of the code from the higher region to the development region for code modifications.	19.07
60	NH	The application should allow for two different versions of the code to reside side-by-side within an environment. In this case, promotion that follows the orderly fashion from a lower environment to the next higher environment should occur but the other version should only be able to be copied into the higher environment (and not be promotable).	19.05
61	HD	The solution provider should provide scripts for promoting code from one environment to the next.	19.09

ID	Type	Requirement	Source
Documentation – Application			
62	HD	The solution should have consistent online documentation and help, with index and search facility for solution management functions, as well as for end-user functions.	9.04
63	HD	The solution should have online screen-sensitive help and topic-based help.	9.05
64	HD	The application should have detailed documentation (online and/or hard copy) of all the possible problems that may occur and the corresponding remedial actions for each problem.	12.09
65	HD	The solution should provide documentation of the application architecture and design. This documentation should be sufficient for training of personnel who will be implementing and managing the application and should include functions, performance, design constraints, and attributes of the software and its external interfaces.	9.01
66	HD	The solution should provide keyboard shortcuts documentation and help.	9.06
67	D	All supporting material should be kept updated with each major revision/version of the application.	22.06
Message Broker			
68	M	The solution shall provide a mechanism to subscribe to external updates in real time. These updates will originate from the statewide information-networking hub.	13.12
69	M	The solution shall adhere to industry standard data exchange format so that external applications can interpret data extracted from the solution. This data exchange mechanism shall be automated (to enable when necessary) and XML-based to conform to the National Information Exchange Model (NIEM) open standards.	13.06
70	HD	The solution should have the ability to integrate with the messaging backbone of the AOC to deliver notifications to the recipients in the event of exceptions and alarms. AOC currently uses Microsoft BizTalk Server.	13.03
71	HD	The solution should have configurable alert creation and notification generation capabilities.	13.04
72	D	The application should provide APIs that support exchanging information with other applications and services in the AOC enterprise architecture.	13.01
Usability			
73	HD	The application should be intuitive to use and relatively easy to learn and use by superior court staff and court clerks.	Usability Service
74	HD	Court administrative staff should be able to set up and schedule a case using the provider solution within an average of 5 minutes. (This is a measurement of how the application allows users to accomplish intended tasks at their intended speed.)	MTG
75	HD	The system should provide a user-friendly graphical interface that makes critical information quickly attainable with a visual sweep on screen.	MTG

ID	Type	Requirement	Source
76	HD	The new system's human interfaces should minimize repetitive motion.	MTG
77	HD	The new system should display descriptive error and other system messages and provide help messages.	
78	HD	Section 508 of the Rehabilitation Act Amendments of 1998 mandates that U.S. government agencies provide access to electronic and information technology to people with disabilities. Vendor must state its degree of compliance with Section 508.	MTG

B. Information Requirements

Information requirements involve the data that the application processes.

The information requirements are organized in the following categories:

- Documentation – Information.
- Information Networking Data Services.
- Interfaces.

ID	Type	Requirement	Source
Documentation – Information			
79	HD	The solution database should contain a comprehensive data dictionary that describes all tables, relationships, data relationship diagrams (entity relationship diagrams), and data elements used in the data structures relevant to court information.	MTG
Information Networking Data Services			
80	M	The provider solution shall provide a mechanism to publish data (through information exchanges with other SOA services) updates on a configurable schedule. The published updates will be used to update the statewide information-networking hub.	13.13
81	HD	Functionality or information provided by the statewide information-networking hub should be accessed in a way that minimizes dependencies on those other systems' implementation details.	13.15
82	HD	The deployment should not constrain central or local configurations.	8.02
83	HD	Functionality or information, which is made available to the statewide information-networking hub, should do so through a software interface that is separate from the system's UI.	13.14

ID	Type	Requirement	Source
Interfaces			
84	D	The solution provider should provide a configurable interface facility that supports input/output table definitions, maps data from input to output tables, splits input records into multiple output tables, combines multiple input records into a single output table, provides logical statements for data selection or conversion, and supports Electronic Data Interchange (EDI) protocols. The interface facility should purge aged (this parameter should be configurable) interface backup transaction files, delete aged interface log files, perform automated interface maintenance, and create batch transaction files.	MTG
85	HD	To allow AOC/ISD to build interfaces between the proposed system and existing systems, Vendor should provide AOC/ISD with the following: <ul style="list-style-type: none"> • Software development kit (SDK) with documentation. • Web services. • Web Services Description Language (WSDL). • Rules engine. • Database schema. • Entity relationship diagram – including referential integrity. • Metadata documentation. • Documented database procedures. • Other vendor documentation to support data access. 	MTG
86	D	The proposed system should provide open, documented interface information in support of future requirements.	MTG
87	D	The system should be able to define and manage interfaces in terms of the data content, context, schedule, and business rules.	MTG
88	D	The provider solution (interface facility) should be able to dynamically initiate appropriate processes when incoming interface data is detected. The data should be validated and appropriate business processes and work flows initiated.	MTG

C. Infrastructure Requirements

Infrastructure requirements involve the physical computer environment that is implemented to support the business application.

The infrastructure requirements are organized into the following categories:

- Database Services.
- Documentation – Infrastructure.
- Hardware and Operating System.
- Monitoring Services.
- Network Services.
- Performance.
- Reliability and Recoverability Services.

ID	Type	Requirement	Source
Database Services			
89	M	All business data shall be stored in a relational database management solution.	7.01
90	M	The database management solution shall be either DB2 or SQL Server.	7.02
91	HD	Direct access to the database should only be performed thru data services such as data transformation objects that abstract the physical database from business services.	7.03
92	HD	The proposed new system should accommodate historical data.	MTG
93	HD	The database should allow extension of both tables and columns based on configuration definition.	10.03
Documentation - Infrastructure			
94	HD	The solution should contain documentation of the technology infrastructure that has been implemented to support the application and business operations. This should include the configuration of the infrastructure. It should also include the procedures required to operate the systems (backups, restart, data maintenance, etc.).	MTG
Hardware and Operating Systems			
95	M	The solution shall operate on one of the following systems: z/OS, UNIX, Linux, or Windows.	16.01
96	HD	All vendor-proposed server software must be multi-tasking and support concurrent multiple users.	MTG
97	HD	Server configuration – AOC/ISD standards include Windows Server, .Net server and software on an Intel based platform. Vendor should provide the minimum Windows or equivalent RECOMMENDED server configuration for installation and operation. Vendor should include the following information: <ul style="list-style-type: none"> • Minimum recommended memory requirements (i.e., RAM). • Minimum recommended storage requirements (i.e., hard disk space). • Supported server operating system. • Minimum recommended server speed. • Standard industry GUI. • Server performance expectations. • Support for retrieval to and from near line storage devices. • Compatibility in a Citrix terminal server environment. • Integrated Windows 2008 domain security. • Any other applicable information. • Indication whether a dedicated server is required. 	
98	HD	The solution should support Virtual Machine standard architecture.	16.02
Monitoring Services			
99	M	The solution shall provide state preservation so that critical information is not lost during failover mechanism.	4.03
100	M	The solution shall maintain a record of changes made to data through a transaction audit file. The audit file shall include the individual user account and the data modified.	3.01

ID	Type	Requirement	Source
101	D	The solution should have a unified management console.	12.04
102	HD	There should be a management dashboard to monitor and manage the performance parameters.	15.02 Infra-structure
103	HD	The solution should allow session monitoring, automatic log file scanning including database logs, and analytical capability of log files.	14.01
104	D	Administration tool – the system should accommodate the ability to create and manipulate the UI without code changes via a centralized management tool.	MTG
105	D	The technical infrastructure servers, databases, and networks should have monitoring appliances and software that permit technical operations staff to monitor the system operations and performance.	MTG
Network Services			
106	M	Internet Information Services (IIS) is the entry point for all external and internal Web service requests. Communication with IIS should use the Simple Object Access Protocol (SOAP) over the HyperText Transport Protocol Secure (HTTPS).	13.08
107	M	The solution shall be compatible with the AOC telecommunications networks. Court staff shall be able to access the application using the current AOC network services.	MTG
Performance			
108	M	The solution shall be able to provide optimum performance through an industry standard solution stack, which is SOAP.	15.01
109	M	The solution shall have a predictable capacity for a specified transaction rate, database hardware, software, and network configuration.	5.01
110	HD	The solution shall have the capability to be available 24x7. The exception is normally scheduled support windows for maintenance, backups, etc.	4.01
111	HD	The screen response time should not exceed 2 seconds.	15.03
112	HD	Operational management of the solution should be through a solution management framework that includes solution operation, monitoring of resource utilization, and performance, as well as control through a browser-based management console.	15.04
113	HD	The solution should be able to grow over time as more users and data are defined to the solution.	20.02
114	HD	The solution should be able to take up the solution load in terms of rise in both transaction and user volume. It should have enough headroom to include vertical capacity and openness to accommodate horizontal capacity without any solution downtime.	20.01
115	HD	The solution should have a documented capacity management plan.	5.02
Reliability and Recoverability Services			
116	M	The system shall be able to determine where it left off during a failure.	18.03

ID	Type	Requirement	Source
117	M	The recovery strategy shall fit within the existing AOC Disaster Recovery Tier 1 requirements.	18.02
118	M	The solution shall have a reliable and documented backup-restoration strategy that is configurable and simple.	18.01
119	M	The architecture of the solution shall ensure No Single Point of Failure (NSPOF).	4.02
120	D	The application should be able to be shut down within a short duration (3 minutes) if there is a need for it.	12.05
121	HD	The system recovery should have automated processes for recovery procedures.	18.04
122	HD	When a system interruption occurs, transactions should be recovered or the database rolled back to a known point with no loss of data or input.	18.05
123	HD	The application should have automatic logging functionality built in to log any problem or error that may occur at any time during normal operation. This log should be human readable and be able to be saved into a text or Word document.	12.11
124	HD	When any problem occurs, whether in hardware or in software, the application/solution should generate automatic e-mail messages to a pre-established e-mail group, notifying them of the problem with sufficient eye-readable and comprehensible details of the problem and the location where the problem arose or resides. Where possible, instructions for remedial action should also be included in the message.	12.08
125	HD	Data and sessions should be recoverable after a shutdown (scheduled or otherwise). Users should not have to do rework.	11.09
126	HD	The application should be able to be started within a short duration (3 minutes) after a shutdown.	12.06

D. Security Requirements

Security requirements are the capabilities required to protect private and operational data from inappropriate access and use.

The security requirements are organized in the following categories:

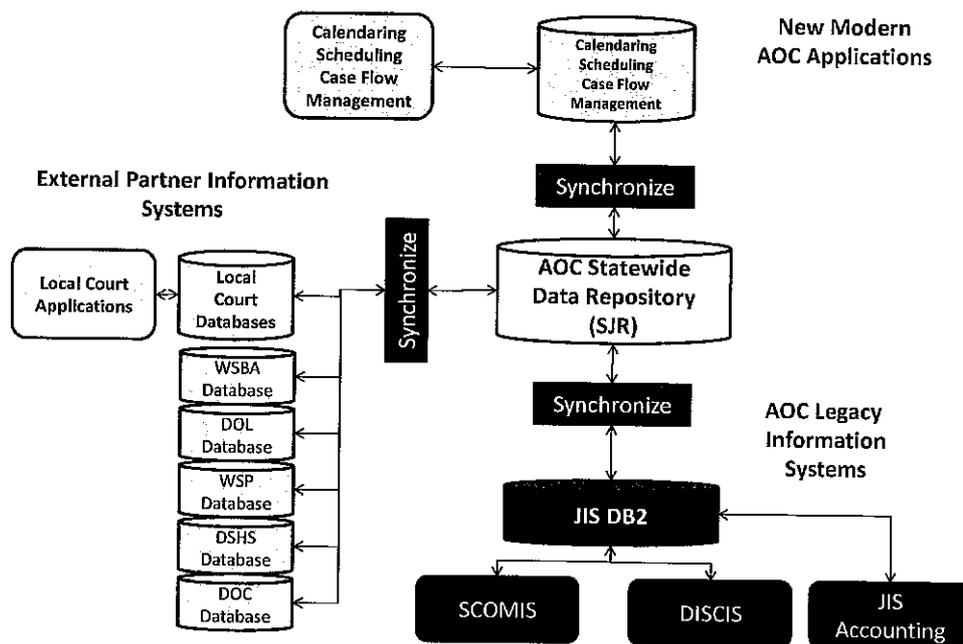
- Access Control.
- Application Security.
- Data Security.
- Documentation – Security.
- Identity Management.
- Network System Security.

ID	Type	Requirement	Source
Access Control			
127	M	Security administration must be available to administrators on and offsite in order to assist with profile authorizations/account updates and password assistance/administration at any given time.	21.13
128	M	For critical data communication between the AOC and the courts, the solution shall support certificate-based authentication using a standard public key infrastructure.	21.03
129	M	For access control, the solution shall comply with user data management, as in a third-party Lightweight Directory Access Protocol (LDAP) security structure.	21.02
130	HD	The application should allow delegation of user management by group or functional role.	12.03
131	HD	The system should maintain an audit log of all access activity to the system. The functionality should allow auditability of security access.	MTG
Application Security			
132	M	Authentication and authorizations shall happen upon initial sign-on and pass seamlessly to all areas of the application without prompting for additional credentials.	21.12
133	D	The unified personalized view of the solution should be controlled.	21.11
Data Security			
134	M	The database shall provide row- and column-level security.	21.04
135	M	The solution shall have the ability to encrypt communications and transmissions between the computing services within and outside the domain of the AOC.	21.01
Documentation - Security			
136	D	The solution should contain documentation explaining the security management approach and the security configuration in the system.	MTG
Identity Management			
137	M	User roles shall determine access privileges and authorization to different functional attributes of the solution.	21.08
138	M	An identity management framework shall control the profiles under specific groups and corresponding policies (external public, court clerk, judicial officer, attorneys, law enforcement, etc.).	21.09
139	D	User profiles shall determine access and privileges to the designated services in the authorization record with the identity management solution.	21.10
Network System Security			
140	M	All incoming and outgoing messages to and from external sources are required to be programmatically encrypted and signed by the sending application using an X.509 certificate.	13.09
141	HD	The solution should provide adequate network system security to protect private and confidential information.	MTG

III. Data Dependencies

New applications that AOC selects to support Washington Superior Court operations will need to integrate with existing JIS applications and database capabilities. AOC plans to implement an enterprise architecture with an information networking hub at its center. The information networking hub will consist of a new Statewide Data Repository (SDR) and a variety of information services. The SDR will maintain information about the entities (persons, locations, attorneys, judicial officers, etc.) case information, and registry of action information (docket). The statewide repository will support judicial applications throughout the state, as well as information exchanges with other external partners (Department of Licensing [DOL], Washington State Patrol [WSP], Department of Social and Health Services [DSHS], etc.). This new SDR repository will replace the JIS database as the statewide repository. The figure below depicts this new architectural approach.

Information Networking Hub



Current, future, and external applications will exchange information with the SDR. When an event occurs that includes data that is of statewide interest, the data will be sent or received from the SDR.

The approach for developing the data dependencies is to examine the business process diagrams, developed in the business requirements process, to locate points of integration. The creation of entity data and start and completion of case cycles, which spawned business information that is relevant to the JIS, is the source for these integration points. In addition, inclusion of any items that need to be recorded in the Register of Actions (docket) or used elsewhere in the portfolio of applications will also be required.

The technology implication regarding the enterprise architecture is that these integration points should follow the publish and subscribe messaging data interchange service defined in the SOA.

A few local applications (King County, etc.) maintain data exchange interfaces with the Superior Court Management Information System (SCOMIS). This allows statewide access to judicial information by all superior courts, statewide.

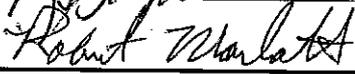
ID	Dependency	Context	Reference
1	Organization types – AOC responsibility. <ul style="list-style-type: none"> • Jurisdiction. • Educational institution. • Law enforcement agency. • School district buildings. • State, county, city. • Out-of-state agency. • Detention facility. 	Organization changes to standard look-up data.	Person data business process diagrams (BPD).
2	Add/modify organization – local courts. <ul style="list-style-type: none"> • Bank. • Collection agency. • Government agency. • Service providers. • Other organizations. • Juvenile unit. 	Add/modify organization.	Person data BPD.
3	Official types – local courts. <ul style="list-style-type: none"> • Add/modify/remove official. • Add/modify/remove law enforcement officer. • Maintain official type (attorney and court administrator data). 	Official types – local courts.	Person data BPD.
4	Juvenile and family. <ul style="list-style-type: none"> • Create new person in JIS. • Select matching person. • Select juvenile. • Link person to juvenile. • Search JIS for duplicate name. • Copy from DOL to JIS. 	Initiated from juvenile referral.	Person data BPD.
5	Well defined person. <ul style="list-style-type: none"> • Search JIS for duplicate name. • Copy from DOL to JIS. • Create new person in JIS. • Select matching person. 	Initiated from charging papers and supporting documents.	Person data BPD.
6	Civil cases (non-criminal). <ul style="list-style-type: none"> • Case added. 	Civil case filed with court or case initiated in SCOMIS.	Person data BPD.

ID	Dependency	Context	Reference
7	Expunge person from case data tables and delete person from person data tables. <ul style="list-style-type: none"> Expunge person from case. Expunge parent from case. Remove person from person database. 	Signed court order. Expunge truancy case or parent eligibility case.	Person data BPD.
8	Delete JIS person. <ul style="list-style-type: none"> Find person in JIS. Delete person in JIS. 	Court order. RCW 13.50.050.	Person data BPD.
9	Maintain attorney. <ul style="list-style-type: none"> Update attorney data. Create attorney or pro se litigant. Update guardian. Add arbitrator data. 	Attorney data extract.	Person data BPD.
10	Arbitrator (non-JIS database). <ul style="list-style-type: none"> File case. Enter arbitrators into system. Select/enter arbitrator. 	Filing case papers – arbitration.	Person data BPD.
11	Interpreters (non-JIS database). <ul style="list-style-type: none"> Add interpreter to list. Update continuing education. 	Need interpreter.	Person data BPD.
12	Guardians (non-JIS database). <ul style="list-style-type: none"> Process application. Process grievance. Appoint guardian. 	Guardian application. Guardian grievance.	Person data BPD.
13	Guardian firms (non-JIS database). <ul style="list-style-type: none"> Process application. Assign guardians to firms. 	Guardian firm application.	Person data BPD.
14	Initiate case. <ul style="list-style-type: none"> Create/update case. 	All case types.	BPD 1.4.
15	Record judgment on case.	All case types.	BPD 1.17.
16	Record treatment plan.	Upon case resolution.	BPD 1.14.
17	Record sentencing information.	Upon case resolution.	BPD 1.22.
18	Post-adjudication processes. <ul style="list-style-type: none"> Modification hearing. Modification requests. 	Upon case modification.	BPD 1.26. BPD 1.25.
19	Close case. <ul style="list-style-type: none"> Case resolution. Case closure (resolution completion). 	Upon case closure.	BPD 1.18.
20	Financial transactions. <ul style="list-style-type: none"> Record financial obligation. Record payments. 	Financial transactions.	(Out of scope.)

ID	Dependency	Context	Reference
21	Record proceeding. <ul style="list-style-type: none">• Create/modify/delete court proceeding.• Assign court staff, court resources, and judicial officers to court proceedings.	Court calendaring.	
22	Register activity in SCOMIS docket.		

IV. Document Approval

Reviewed by:

Title	Name	Signature	Date
Project Sponsor	Vonnie Diseth		3/11/2011
MTG Project Officer	Joseph Wheeler		3/4/11
AOC Project Manager	Kate Kruller		3-4-11
MTG Project Lead	Robert Marlatt		3-4-11