APPENDIX C.   DMS TECHNICAL REQUIREMENTS

C.1   INTRODUCTION

This appendix is an overview of the California Judicial Branch infrastructure and technical requirements considerations that require a written response. The considerations given in this section should be used when crafting a proposed solution.

C.2   GENERAL INSTRUCTIONS

Using approximately a page for each, describe how the proposed solution addresses the subsections listed in the table below, paying particular attention to the concerns listed in the table column across from the section. Any compatibility or supportability concerns or any non-compliance of the solution with any of the considerations listed in this section should be specifically called out and explained.

C.3.1	Discuss how and to what extent the solution complies with United States Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0. When describing compliance, distinguish whether an accessibility feature is incorporated within the product suite or compatible with third-party user-assistive technology. Also address any tools or features that will assist the branch in managing and assessing the compliance of content with Section 508 and WCAG.
C.3.2	Describe how the solution supports Administrative Office of the Courts Layered Security Architecture, platforms and virtualization; and the vendor experience with managed environments similar to the California Court Technology Center.
C.3.3	Specifically list and describe any required client-side or desktop system plug-ins or ActiveX controls.
C.3.4	Include typical deployment reference architecture and describe how the proposed solution will address the variety of deployment alternatives within the California Judicial Branch.
C.3.5	Explain how the solution will address security concerns for installations without a shared security service; and the solution compatibility and support for the Oracle Security Suite and Microsoft Active Directory.
C.3.6	Describe how the solution supports integration and interoperability with existing DMS and automated systems within the branch, and specifically: 1. List and describe any plug-ins or integration interfaces to third-party systems, particularly: SAP and Oracle Financials. 2. Describe one of more examples of past integrations with SAP and Oracle Financials. 3. Describe the solution support for open standards like Content Management Interoperability Services, Web Services for Remote Portals, JSR168 and JSR263; and other web service and Service Oriented Architecture standards. 4. Discuss how the solution supports branch case management systems (CMS) functionality, particularly the batch exchange of documents, metadata and security with CMS. 5. Describe the solution Application Programmer's Interface (API), web service interface, or other mechanism that exposes DMS functionality to clients.

Project Title: Judicial Branch Enterprise Document Management System
RFP Number: FIN122210CK

APPENDIX C. DMS TECHNICAL REQUIREMENTS

C.3   CONSIDERATIONS

Systems and applications that may be hosted by the Administrative Office of the Courts (AOC) on behalf of the Judicial Branch are subject to a number of technical requirements listed in this document that should be considered when proposing a solution. These requirements should be incorporated into the solution architecture even though larger county courts that host installations separate from AOC may relax or eliminate certain technical requirements, or impose others.

C.3.1   Accessibility Compliance

Compliance with United States Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0 is a goal of the Judicial Branch. The branch requires solutions that are Section 508 and WCAG complaint; and that offer content compliance management and compliance monitoring tools, and other features, that will assist the branch in meeting its accessibility objectives.

C.3.2   California Court Technology Center (CCTC)

The California Court Technology Center (CCTC) is managed by the Information Services Division (ISD) of the AOC and offers centrally hosted shared managed services for use by the Courts. CCTC is a Tier 3 data center, with geographically separated production and disaster recovery infrastructure.

Production applications used by the AOC or offered on behalf of the California Courts are hosted from CCTC and are subject to certain specialized requirements, including High Availability, disaster recovery, Layered Security Architecture compliance, and limitations on deployed systems and platforms.

C.3.2.1 Layered Security Architecture

ISD Layered Security Architecture (LSA) is an application of "defense in depth" intended to enforce enclave boundaries using firewalls. Compliance with LSA requires an application architecture consisting of a minimum of four tiers: proxy, presentation, application, and data [base]. Each of the fours tiers is separated with firewalls. Strict segregation between development, test, staging and production environments is also enforced.

Compliance with LSA is mandatory for applications deployed at CCTC.

APPENDIX C. DMS TECHNICAL REQUIREMENTS

C.3.2.2 Supported Platforms

Applications hosted from CCTC are deployed on either Sun Solaris Unix or Intel Microsoft Windows. Databases are Oracle or preferably Oracle Real Application Cluster (RAC).

No other platforms are currently supported.

C.3.2.3 Virtualization

Services may be offered from virtualized infrastructure when appropriate and compatibility with Oracle Sun or VMWare virtualization technologies is strongly preferred.

C.3.3 Client-Side Plug-Ins

In order to reduce or eliminate changes to deployed desktop infrastructure, the Judicial Branch prefers no required client-side plug-ins or ActiveX controls. However, plug-ins may be considered when the functional requirements or the technical requirements of the solution cannot be satisfied using another mechanism. In general, specialized custom coded plug-ins or specialized custom coded ActiveX controls will not be acceptable to the Judicial Branch.

C.3.4 Deployment Architecture

There are three likely deployment alternatives for California Judicial Branch installations:

1. Hosted within the CCTC used by the AOC and shared with other county courts.

2. Hosted by a larger county court and shared with other county courts.

3. Hosted by a county court for internal use only.

C.3.5 Security Services

AOC intends to utilize a shared security service for authentication and authorization; however, some court installations may lack this capability. In the latter case it is expected that the solution will provide authentication and authorization services without reliance on an existing security service.

C.3.5.1 Oracle Security Suite

The AOC is currently implementing the Oracle Security Suite shared security service. The components of the Oracle Security Suite anticipated by AOC at CCTC are:

- Oracle Internet Directory (OID)
- Oracle Virtual Directory (OVD)
- Oracle Identity Federation (OIF)

APPENDIX C. DMS TECHNICAL REQUIREMENTS

- Oracle Access Manager (OAM)

Oracle Security Suite augments authentication services offered by Microsoft Active Directory.

C.3.6 Service Oriented Architecture

Integration with existing and future case management systems and other applications and systems is a key goal of the branch. Supporting this goal mandates solutions that expose functionality using web services, and open standards compliance, including:

- File Transfer Protocol Secure (FTPS)
- Hypertext Transfer Protocol (HTTP)
- HTTP Secure (HTTPS)
- Secure Shell (SSH) File Transfer Protocol (SFTP)
- Simple Object Access Protocol (SOAP) 1.2
- Universal Description, Discovery and Integration (UDDI)
- Web Services Description Language (WSDL)

- Content Management Interoperability Services (CMIS)
- Web Services for Remote Portlets (WSRP)

C.3.6.1 Integration Services Bus

Using the TIBCO platform and Oracle Web Services Manager (OWSM), AOC has implemented a set of reusable common services that provide logging and exception handling, and inter-system data exchange. These services are collectively referred to as the Integration Services Bus (ISB).

For solutions hosted from CCTC, ISB must mediate the exchange of information with other systems.

C.3.6.2 Enterprise Systems Integration

Automated systems are employed for a variety of enterprise functions. SAP supports finance, human resources and benefits administration. Oracle financials supports central accounting functions. Computer Aided Facilities Management (CAFM) by TRIRIGA supports Computer Aided Design (CAD) and facilities management. Additionally, a variety of DMS already exist within the branch. Finally, the business of the Judicial Branch requires extensive automation provided by a variety of Case Management Systems (CMS) including: Sustain, V2, V3 and California Case Management System (CCMS). There are also internal portals and public facing external portals offering information services to consumers.

APPENDIX C. DMS TECHNICAL REQUIREMENTS

Although CCMS houses a document store and performs internal document management, DMS back-end services are also required. The exchange of metadata between DMS and CMS occurs predominately in periodic batch exchanges.

Whether through web services, open standards, or proprietary API, solutions integration with existing automated systems is a branch-wide concern. Additionally, WSRP, JSR168 and JSR286 compliance is preferred.