Attachment 1

Current AOC Networking and Computing Environment

1.1 The Administrative Office of the Courts (AOC) seeks information that may provide a solution that will integrate well with the existing technical architecture. Additionally, the solution should be scalable to support continued growth of the California Judicial Branch (Branch) throughout the state.

1.2 The majority of the Branch is using Microsoft Exchange 2003 as well as the Microsoft Office professional suite of applications (Word, Excel, etc) for office automation. However, Microsoft Exchange is not an established standard and some courts are using other products. The AOC is migrating to the Windows 7 Client operating system.

1.3 The solution needs to integrate with existing DMS solutions already deployed throughout the Branch.

1.4 The AOC has developed a centrally hosted shared services model with an outsourced co-location facility California Court Technology Center (CCTC) where all servers are to be hosted in a highly available and secure manner. The Managed Service Provider has standardized monitoring with BMC patrol and a preferred solution will include integration with the implemented monitoring toolset. Larger trial Courts may have locally hosted deployments with customized toolsets.

1.5 The solution will be highly available with a redundant infrastructure that supports automated failover in case of component failure. Load sharing based solutions are preferable over hot standbys. As part of the co-location's business contingency strategy, there is a secondary site for Disaster Recovery (DR). The DR strategy relies heavily on Storage Area Network (SAN) to (SAN) data replication, so a solution that would allow utilizing the existing solution would be preferred.

1.6 The network connecting the different business units (AOC, trial/appellate courts and others) is an IP network hub and spoke model with leased lines between the co-location facility and the offices. The AOC has standardized on a Cisco Network infrastructure.

1.7 The current identity management solution implemented within the co-location facility is based on Oracle's suite of security products to provide a standard solution for user authentication. It is important that all new solutions implemented are fully integrated to work with the security framework designed at the co-location facility and can operate within a federated security model. The DMS vendor will be responsible to prove the integration and support it as part of the maintenance of the DMS product.

Attachment 1

Current AOC Networking and Computing Environment

1.8 The AOC, California Supreme Court and Courts of Appeal are trying to standardize on Microsoft and Sun Solaris Unix based solutions with off the shelf or original equipment manufacturer (OEM) products customized to the AOC environment.

1.9 Oracle is the preferred choice of the AOC for relational database management. Other database solutions are currently used as part of the core AOC hosted service offering, but in an effort to standardize, any solution that supports the most current version of Oracle in a multi-host real application clustering implementation will be preferred.

1.10 The solution needs to be capable of seamlessly integrating into our Integrated Service Backbone (ISB) for exchanging data to and from any other systems hosted either within the co-location facility or externally in local Court document management system. The AOC has implemented the Integrated Services Backbone based on the product suite from TIBCO. A solution that has a J2EE, Java API and exposes its functionality with web-services will be preferred.

1.11 The AOC utilizes an enterprise level EMC solution for centralized storage (storage area network) that should be used for any storage of live data. The Managed Service Provider is utilizing standard enterprise solutions for backups and restores.

1.12 The AOC will seek a solution that can be implemented in an n-tier environment with a thin client front-end. The proposed solution must be able to operate in a 'defense in depth' infrastructure environment.

1.13 All communication between clients and applications needs to be HTTPS.