Attachment 13

Features List: Architecture, Infra, & Security

| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Preferred | N-Tiered Architecture | Application architecture shall consist of a minimum of four tiers: proxy, presentation, application, and data [base]. Each of the fours tiers shall be separated with firewalls. Describe how the application architecture supports n-tiered Architecture. | | |
| Info Only | Accessibility | Discuss how and to what extent the solution complies with United States Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0. | | |
| Preferred | Plug-ins / Active X controls | 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. Specifically list and describe any required client-side or desktop system plug-ins or ActiveX controls. | | |
| Info Only | Operating Systems | Specify list of supported operating systems and their versions. | | |
| Info Only | Oracle Database | Judicial Branch has enterprise license for Oracle database. Specify support for Oracle Database 11gR2 or later.  List all supported versions. | | |
| Info Only | Oracle RAC | Specify support for Oracle Real Application Cluster (RAC) | | |
| Info Only | Virtualization | Specify the list of virtualization technologies supported. | | |
| Preferred | LDAP-v3 | Application shall support LDAP-v3 compliant directories for authentication. | | |
| Info Only | Other authentication | Specify supported authentication methods. | | |
| Preferred | Authentication at Presentation Layer | User sessions shall not be allowed beyond presentation tier without authentication. Authentication shall be at the web server (presentation layer) | | |
| Mandatory | Network Traffic Encryption | All network traffic between the browser and the application shall be encrypted. | | |
| Mandatory | High Availability | Application shall function in an active-active High Availability configuration without any single point of failure in any of the application components. Describe High Availability architecture of the application. | | |
| Preferred | Core & Public application independence | Publicly exposed application shall not impact Core application used by court users. Publicly exposed application shall be deployed separately with no shared components with Core application. Describe the architecture of Core and publicly exposed application. | | |
| Info Only | Supported Web Servers | List the supported Web Servers and their versions. | | |

Attachment 13

Features List: Architecture, Infra, & Security

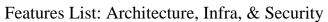| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Preferred | Web Browsers | Microsoft Internet Explorer version 7 or later is used at the courts.  Support for the IE browser is highly desirable.<br>List all supported browsers and versions. | | |
| Info Only | Configuration update method | Describe how court configuration is updated in the application. | | |
| Mandatory | Firewall Port Numbers | The product shall list all port numbers for proper firewall configuration | | |
| Info Only | Identity Propagation | Describe how user credentials and user context are propagated to any integration point outside application server including to the database. | | |
| Mandatory | Application Network Traffic Encryption | All incoming and outgoing network traffic of the application shall be encrypted. | | |
| Mandatory | Encryption of Sensive Data | All sensitive data stored in the database shall be secured and encrypted. | | |
| Preferred | PCI Compliance | Application shall comply with Payment Card Industry (PCI) security standards. | | |
| Preferred | Horizontal Scalability | Application must be horizontally scalable | | |
| Preferred | Vertical Scalability | Application must be vertically scalable | | |
| Preferred | Web Traffic Compression | Application shall function with compression enabled at Web Server level. | | |
| Info Only | Network Bandwidth | Specify network bandwidth requierments with & without compression enabled at the web server level. | | |
| Preferred | Recommended Infrastructure | Vendor shall have recommended specifications available for Server/CPU/Memory/Storage/Network resources for given number of users in active-active High Availability configuration as well as non High Availability configuration | | |
| Preferred | Performance/Stress Test Results | Provide comprehensive performance/stress test and results documentation. | | |
| Info Only | 32 / 64 bit | Describe support for 32bit and 64bit operating systems | | |
| Preferred | Web Services Protocols | Integration with existing 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:<br>• File Transfer Protocol Secure (FTPS)<br>• Hypertext Transfer Protocol (HTTP)<br>• HTTP Secure (HTTPS)<br>• Secure Shell (SSH) File Transfer Protocol (SFTP)<br>• Simple Object Access Protocol (SOAP) 1.2<br>• Universal Description, Discovery and Integration (UDDI)<br>• Web Services Description Language (WSDL)<br>Describe support for the listed open standards | | |

Attachment 13
Features List: Architecture, Infra, & Security

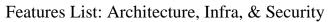| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Preferred | Web Services Security | Support for WS-Security, Certificate based security, Basic HTTP authentication and SAML standards are highly desired.<br>Describe supported authentication methods for Web Services | | |
| Info Only | Reports Architecture | Describe the reports architecture | | |
| Info Only | Adhoc Reports Architecture | Describe ad-hoc reports architecture | | |
| Info Only | Reporting Database | For reports, if a separate reporting database is required, describe the supported data replication mechanisms. | | |
| Preferred | Static Content | For application efficiency all non-secure static content must be served from web server. | | |
| Info Only | Web Service Interoperability | Describe compliance with the WS-I (Web Service Interoperability) specification | | |
| Preferred | Web Browser only | Application should be accessible via a web browser without users having to install program components to the local desktop. | | |
| Mandatory | Application Logs | Application shall support logging for information, and debug purposes at Web Server, and Application layer components. | | |
| Preferred | Application Log Details | Application logs shall have userid, sessionID, timestamp, request URI and response times for requests. | | |
| Preferred | Response Time information | Capturing and displaying end-to-end response times for interactive user requests is highly desired. | | |
| Preferred | Cleanup | Application shall provide functionality to cleanup temporary data, files, and any other temporary stale information. | | |
| Preferred | Security-Malicious Content | All input (via web services or user entered) shall be scanned for malicious code before processing or storing in the Database. | | |
| Info Only | Security-Malicious Content Testing | Describe how the application is tested against security vulnerabilities (cross site scripting, SQL injection, buffer overflow, malicious input, etc) | | |
| Info Only | Security-Application | The Open Web Application Security Project (OWASP https://www.owasp.org/images/4/4e/OWASP_ASVS_2009_Web_App_Std_Release.pdf) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. OWASP Application Security Verification Standard (ASVS) is used to establish a level of confidence in the security of Web applications.<br>Describe the applications' adherence to OWASP-ASVS standard and the results of the security verification. | | |
| Info Only | Third Party Tools | Describe any third party tools requiring licenses to run the application | | |
| Info Only | Batch Jobs | Describe the batch job architecture. | | |
| Preferred | Batch Job Documentation | Documentation shall be made available for each batch job, with its detail descriptions, parameters, recommended running time, approximate expected run time, and natural design dependencies on other batch jobs. | | |

## Attachment 13
### Features List: Architecture, Infra, & Security

| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Info Only | DMS Integration | Judicial Branch has selected Documentum and FileNet as Document Management System vendors.<br>Describe out-of-box integration with Documentum and FileNet. | | |
| Info Only | Batch Job Dependency | Describe the ability to handle dependencies between batch jobs | | |
| Preferred | Batch Job Failure | Restarting a failed batch job shall start where the previous instance stalled. | | |
| Info Only | Batch jobs processing large amount of data | Describe how processing of large amount of data is handled in batch jobs. | | |
| Preferred | Authentication | Once the user authenticated at the Web Server (presentation tier) level the application shall not prompt for authentication again. | | |
| Preferred | Session Timeouts | Session duration shall be configurable | | |
| Preferred | Application Server Access | Users, API or services must not be able to access Application Server directly without being authenticated at the Web Server layer. | | |
| Mandatory | Authentication Token Validity | Once authenticated at the Web Server, the authentication token passed in to Application Server must be asserted with the Security Policy Server for validity | | |
| Preferred | RBAC | Application shall support Role Based Access Control for users and Web Services | | |
| Info Only | Auditing Arch | Describe auditing architecture. | | |
| Info Only | Large Case Records | Describe how cases with large number (> 1000) of participants are handled in the application | | |
| Info Only | Infrastructure | To reduce capital and operational costs it is highly desirable to run multiple non-production environments on the same infrastructure/hardware.<br>Describe how the application supports multiple instances in such an environment. | | |
| Preferred | Web Services API | All API exposed for integration with other application shall be Web Services conforming to Industry Standards | | |
| Info Only | Infrastructure Non-HA | Non production environments may use infrastructure without HA.<br>Describe the application architecture without High Availability. | | |
| Info Only | Infrastructure - Supported Hardware | Describe the supported hardware configurations | | |
| Info Only | WebLogic | Judicial Branch has branchwide license for WebLogic application server.<br>If the proposed solution is a Java EE based solution, specify support for WebLogic application server and the supported versions. | | |
| Preferred | Equipment Specifications | Necessary systems and hardware must not be proprietary in nature and have ability to be "racked" in standard 19" four-post server room racks. | | |

Attachment 13

Features List: Architecture, Infra, & Security

| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Preferred | Application/Equipment and Monitoring | Ability for applications and processes to be monitored and performance measured using industry standand monitoring tools such as Solarwinds | | |
| Mandatory | Windows environment compatible | Ability to operate in a Microsoft Windows server and desktop environment. | | |
| | | | | |
| Preferred | Virtualization | Ability to operate in a standard virtualized environment such as VMWare Enterprise | | |
| Desired | AD Integration | Ability to integrate with existing Active Directory for security and authentication | | |
| Preferred | Equipment Specifications | Necessary systems and hardware must not be proprietary in nature and have ability to be "racked" in standard 19" four-post server room racks. | | |
| Preferred | Scalability and Redundancy | Ability of system to scale to multiple servers for purposes of redundancy and load expansion | | |
| Mandatory | Network Requirements | Ability to operate on standard, static IP based (IPv4, capable of upgrading to IPv6) network with varying circuit types and bandwidths (i.e. T-1, DS3, etc.) | | |
| Preferred | Application/Equipment and Monitoring | Ability for applications and processes to be monitored and performance measured using industry standand monitoring tools such as Solarwinds | | |
| Mandatory | Windows environment compatible | Ability to operate in a Microsoft Windows server and desktop environment. | | |
| Preferred | Database Support | Ability to operate utilizing common, non-proprietary database platforms including Microsoft SQL Server and/or MySQL | | |
| Preferred | Power Requirements | Power requirements should be 110V AC 60hz with ability to have dual redundant power supplies | | |
| Preferred | Application Backup & Restoration | Ability for software and data to be backed and stored using industry standard software and media such as Tivoli | | |

Attachment 13

Features List: Architecture, Infra, & Security

| Priority | Requirement Name | Requirement Text | Response | Comment |
|---|---|---|---|---|
| Preferred | Server specifications | Ability to system and software to operate on industry standard servers, preferably Dell. Ability to have all equipment covered by same day maintenance contract. | | |