SYSTEM WIDE ARCHITECTURE COMMITTEE

CALIFORNIA COMMUNITY COLLEGES

Recommended RFP Questions to Support System Standards

Version History

Version #	Date	Author	Key Differences
DRAFT	5/25/2017	Tim Calhoon	Initial Draft

FINANCIAL & ORGANIZATIONAL STABILITY OF PROPOSER

Provide the legal company/organization name.

Provide the number and location of your businesses offices.

What was the year the organization was founded?

What is the legal form of the organization? (i.e., sole proprietorship, partnership, LLC, corporation/state of incorporation)

What are the organization's principal lines of business?

Describe the organization's governance structure.

Did the organization produced a profit, or sustainable reserve (if a non-profit) during the last fiscal year?

Has the organization consistently shown a profit for each of the last five fiscal years? Describe any circumstances, time frame, and resolution surrounding a lack of consistent profitability or sustainable reserve.

Has the organization ever filed for bankruptcy? Describe any circumstances, time frame, and resolution surrounding a bankruptcy.

Are audited annual reports available to potential clients?

Disclose any conditions (e.g., bankruptcy or other financial problems, pending litigation, planned office closures, impending merger or sales of the company) that may affect your firm's ability to perform contractually.

Are you currently in litigation with a customer?

Has the organization been engaged in a lawsuit with a customer and the customer won the lawsuit?

How many employees, not including contractors, are currently employed by the organization?

How many employees has the organization hired over the last 12 months?

How many employees have left the organization over the last 12 months?

What is the average length of service for all of the organization's employees?

Provide a list of current customer references for similar services representing three of the accounts currently serviced. Please list any community colleges and school districts to which your firm has recently provided similar services. For each reference, include the company name and business address; the name, job title, and phone number of a contact person; and a brief description of the service provided and the period of service.

Provide the company, name, telephone number, and email address of accounts that have discontinued their use of your company's products and services in the last 24 months, for reasons other than consolidation.

Information Security

Will the system automatically log out after a period of no activity?

Describe your experience with information security standards including which standards your organization follows related to security, e.g. FERPA, HIPPA, PCI-DSS, etc.

Does your company have a Chief Security Officer? Please list the individual's name and contact information.

Describe your policy and implementation of timely communication to the customer base regarding issues such as outages, bugs, downtime, etc.

Is there a password policy? If yes, please describe. Is two-factor authentication used?

Will the system provide the option to disable user IDs for a configurable time frame after a specified number (configurable) of consecutive invalid login attempts?

Will the system enter passwords in a non-display field?

Will the system encrypt passwords when they are routed over the network?

Will the system provide a method of secure login for students and adults and comprehensive security for all system components?

Will the system provide security for all system components at database, workstation, and individual operator levels?

Will the system provide secure access control based upon single unique user login?

Will the system check each user's access privileges at login, and automatically disable or enable client functions (in real time) based upon the user's profile?

Will the system contain safeguards to prevent release of information without proper consent in order to protect the integrity and confidentiality of data? If yes, please describe.

Will the system provide federated identity management capability?

Will the organization provide and ensure effective physical security measures for all proposed equipment sites, all processing and operations areas, and secured storage areas. If yes, please describe

Is security awareness training in place? If yes, please describe.

Is there an inventory of PII? If yes, please describe.

Is there any background checks performed as a condition to access PII?

Is there a media handling policy? Is there a media disposal policy? If yes, please describe.

Is there an access control policy to grant access to applications and data on an as needed basis? If yes, please describe.

The Proposer must have a current annual security rating from an independent third party auditing firm that certifies that the Proposer meets federal guidelines for the handling of confidential data. If yes, provide self-reported proof or documentation.

What type of authentication do you use for your web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)

Is there a firewall in place in front of your organization's network? If so what type? Who has admin access to it? Who has view access? Are the logs reviewed?

Describe any associated data center buildings and whether they are built to Essential Services standards.

Has any testing been done of the publicly accessible portions of the application to test for common web application vulnerabilities such as the OWASP top 10?

Does your organization's servers share a network with any other organization? If yes, please describe.

Are the network configurations on any of the switches and routers default?

What services do you expose to the Internet?

Does your organization have any systems that use modems? If yes, please describe.

What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)

Is there any type of revision control used? If yes, please describe.

Is there any IDS or IPS products running in front of your organization's Network? If yes, please describe.

Are any file integrity tools such as tripwire used? If yes, please describe.

Does your organization's Servers use host-based firewalls? If so what ports are available?

Does your organization use any Remote Access services, if so which? VPN, SSH, RDP, etc)

What antivirus application(s) do you use?

Is your antivirus application implemented using a "managed" client/server architecture, or in a stand-alone configuration?

Has any automated Vulnerability testing product such as Nessus ever been used to identify know application vulnerabilities?

Do you have a patch management policy? If yes, please describe.

Describe how your servers clocks are synchronized.

Is there a centralized log server? If yes, how often are log files reviewed and what is the process?

Do the systems maintain logs or audit files?

Does the system have any default accounts? If yes, please describe.

Describe how the system will provide end-to-end data protections to ensure no data is lost or corrupted during processing, storage, and transportation between applications and interfaces.

Describe how the system will support the seamless and secure sharing of student information with the respective state-specific student information management systems. This includes both the receipt of student data from the state systems and the export of student results back to the state systems.

Describe any incident in which your organization's network may have exposed Personally Identifiable Information (PII).

Describe your process for accessing data following a contract termination.

What are your data retention policies, historical archiving processes, and retrieval of archived data policies? Is data securely deleted at the end of the retention period?

Is all communication between servers encrypted? If so what kind?

Is sensitive data encrypted at rest? If so what kind?

Has a tool such as spider or Identity Finder been used to validate the inventory? If yes, please describe.

Will the system log unauthorized access attempts by date, time, user ID, device, and location?

Will the system maintain an audit trail of all security maintenance performed by date, time, user ID, device, and location, with easy access to information?

Will the system include comprehensive field edits to prevent incomplete or incorrect data from entering the system?

Describe how sufficient audits will be available to identify the source and time of data changes related to system components.

Describe how the system will log system activity necessary to monitor and debug the system in a timely and accurate manner.

Will all errors be written to an error log?

Will errors to the end user be communicated in plain language with an explanation of required action?

Will the system allow for a system administrator to view, filter, sort, and search the error log?

Describe the organization's backup routine.

Briefly describe the organization's Disaster Recovery plan.

Will the Test Delivery System have built-in redundancy and fail-over architecture to ensure seamless system recovery? If yes, please describe how the Test Delivery System will recover from a hardware or application failure.

Describe where your redundant servers are located.

Describe the triggers, and timelines for switchover to redundant servers.

What is the tier level of redundancy that your data center, which will host the proposed system, is certified for?

Will the proposed application support recoverability using commonly available and industry standard backup applications and approaches, including the ability to provide point-in-time recovery of data to the last completed transaction, allow for continued use of the system during backup, and provide a complete backup and recovery process for all database tables and system files?

Can the backup and archival features of the system proposed be initiated automatically or by manual request?

Will the proposed system use real-time replication so that testing is not interrupted during fail-over?

Will the proposed system be able to route data to multiple data centers distributed across the state?

Accessibility

Describe your technical experience in developing information and communication technology products that meets the Web Content Accessibility Guidelines 2.0, Level AA (https://www.w3.org/TR/WCAG20/) standards and the US Section 508 Standards for Information and Communication Technology (https://www.federalregister.gov/d/2017-00395).

How do you ensure that the web applications you develop meet the Web Content Accessibility Guidelines 2.0, Level AA level? Please describe and provide supporting evidence of the processes you follow.

What automated and manual testing do you perform to test and evaluate applications for accessibility for individuals with disabilities? Please describe your testing process in detail.

Does your product undergo accessibility testing prior to each major release? Do you use a third-party accessibility evaluation company to verify your accessibility compliance? If so, are you willing to provide a copy of your most recent evaluation report?

Which assistive technologies on the Windows OS and macOS platforms do you test with in order to evaluate access for blind and visually-impaired individuals?

What is your policy and process for responding to issues identified as an accessibility error for applications in development and production environments? How do you track and prioritize accessibility issues?

What methods do you use to inform customers of accessibility errors?

Do your developers and project managers receive or engage in accessibility training on a regular basis? Please describe the extent of such accessibility trainings.

What percentage of your software development and testing team is focused on accessibility?

Do you have a designated accessibility representative to address issues or questions related to the accessibility of your product?

Support

Please describe why the organization's experience and approach to client engagement would result in a superior partner for development, delivery, and maintenance.

Describe your policy and implementation of timely communication to the customer base regarding issues such as outages, bugs, downtime, etc.

Describe any community support mechanism (i.e., Get Satisfaction) that is integrated with your customer support.

The college provides Help Desk support to various services. Describe how you will interface your Help Desk support with college's and provide access to your ticketing system. Include software tool used to log, track and close tickets.

Describe your support Service Level Agreements (SLAs).

Describe your service level metrics including items like first contact closure rate, average speed to answer, average time to respond to email, call abandonment rate, follow-up on calls due to problem repeated after initial fix failed, and overall Quality Assurance ratings across all clients.

Describe your approach to tracking and measuring customer satisfaction including what reporting is provided back to management.

Describe your company's support Quality Assurance procedures (i.e. steps to provide timely and accurate issue resolution).

Does your company follow the practices of Information Technology Infrastructure Library (ITIL) for defining a common language for service desk management and incident resolution? If not, describe your practice in managing continuity in communications and nomenclature.

Describe your company's process for escalating support issues.

Provide names and titles for escalating level of contact if service levels fall below agreements.

Describe the availability of your call center and help desk for end users and CCC management team.

Describe your policy and implementation of timely communication to the customer base regarding issues such as outages, bugs, downtime, etc.

Do you use any third party contractors to maintain data or applications? If yes, please describe.

Project Management

Describe in detail how your organization intends to address the anticipated scope of work.. Include the project plan that the organization will follow from initial design, to pilot, and through implementation of the finished product. Include specific deliverables and activities that the organization will complete.

Outline the project schedule, including the design, pilot, and implementation phases. Describe the methods that will be used to maintain this schedule. Explain if, and why, the timeline differs from the proposed timeline in the RFP (See Scope of Work).

Provide a description of the organization's structure describing the responsibilities of staff and contractors assigned to the project. Identify the key individual(s) who will act as project lead, project monitoring, and all other professional staff who will work directly with the District and other key stakeholders. Include a description of the experience and qualifications of the key individual(s).

Describe the assignment of deliverables and activities within the organization to complete necessary scope of work. Include a description of the experience and qualifications of the key individual(s) performing the work.

Describe the organization's method for consensus building, including: role, the methodology employed, the outcomes, and a recent project in which the organization successfully employed this method.

Describe the organization's process for the design, review, approval, and completion of essential project elements. Include the editing and feedback process, as well as how the organization would address changes or additions to the scope of work that could occur during this process.

Describe the types of problems the organization has encountered on similar projects, and explain what was done to resolve the problems. How would your organization avoid similar problems on this project?

System Requirements

Will the system function with non-English keyboards?

Describe how the system will incorporate SAML 2.0/Shibboleth to offer single sign on capability for students, faculty, and administration.

Does the organization have the ability to secure and maintain a direct network connection or peering through a CENIC network partner from its hosting environment to the CENIC California Research & Education Network (CalREN)? If yes, please describe.

Describe how the system will minimize latency to institutional SIS systems it achieve as close to "real-time" as possible.

Software Development

How many employees does the organization have in the following areas? Project Management / Software Design and Development / Systems-Network Administration / Quality Assurance / Customer Support / All Others.

What number and percentage of the organization's software developers (including contractors) are living and working within the US?

From what countries outside the US does the organization hire developers as employees or contractors?

Describe the organization's quality and configuration management systems.

Describe your use of and experience with open source software (leverage, contribute, create).

Describe your experience developing and deploying multi-tenancy software.

Describe your experience incorporating standards (IMS, SCORM, etc.) into products.

Describe your experience making software functionality accessible to all students and faculty (Section 508 compliance, etc.)

Describe your experience creating a service oriented architecture (SOA) framework.

What is your software test methodology?

Describe your experience developing product extensions with a client. Include details regarding ownership of source code or intellectual property.

What percent of your regression tests are automated?

Describe your approach to feature testing, release testing, regression testing, and deployment testing.

What is your release model?

Describe whether software updates require downtime, and if so, what is the average duration and frequency of downtime?

Describe your level of experience with and current support of mobile platforms, specifically smart phones using Apple iOS and Android. Please differentiate between your use of native clients, responsive design (single URL), multiple URL (e.g. xxx. and m.xxx.), and general reliance on mobile browsers.

Describe your future Assessment development plans with regard to milestone events (major revisions to the technology stack, functional capabilities, and integration of third party components) of your proposed solution.

Describe all API's, web services, and other support for 3rd party integration including support for extensions by the client.

Describe your company's experience integrating with uPortal or through JSR-168/286 portlets. Provide specific examples.

Describe how you would support a workflow where the system can be configured, tested and deployed by individual colleges in separate steps.

Describe how you determine what the trends are in your development process for new applications and integrations. How do you stay current on trends and regulations?

Describe how the proposed method uses coding standards and code reviews to ensure that the development team follows these coding guidelines to facilitate the readability of the source code and to make software maintenance easier.

- Technology stack, e.g. Windows, Unix / language (Java, etc), web server/app server (IIS, Apache, tomcat), DB server (MS, Oracle, etc.)
- Required licenses not provided with solution (e.g. OS, DB, etc.)
- When was the software initially launched to market?
- If > 5 years ago, list out the dates of major releases
- Identify for every major release whether the software was "re-designed" vs. simply updated.
- Please provide a sample Implementation project plan including major milestones, expected time to complete (average) each phase, and overall average time to implement.
- Do you provide implementation services as part of the license or are they purchased separately?
- Are there any restrictions as to deployment in the cloud? Please list and summarize.

Need standard language to make CCC contracts piggy-backable.