# CITY OF AUSTIN
# Scope of Work
# COMPUTER-AIDED DISPATCH AND RECORD MANAGEMENT SYSTEM WITH INTEGRATED MOBILE & GEOGRAPHIC SYSTEMS

Background

In 2012, the Austin Convention Center Department (ACCD) was host to an estimated 300 meetings, conferences and conventions, and approximately 1,000,000 visitors in and out of the doors of the Austin Convention Center Department and the Palmer Events Center. The ACCD's current physical facilities include the Austin Convention Center, the Palmer Events Center, the African American Culture and Heritage Facility, and the 4 associated parking garages and facilities.

In early 2010, a reorganization of the ACCD's Security and Safety Division was begun. This reorganization focused on an assessment of the then current business practices that supported the security and safety of all hosted events, employees, and physical facilities of ACCD. After the initial assessment was conducted and direction was approved, the Security and Safety Division began program improvements to include development of contemporary best practices, policies and training in the areas of security, safety, asset protection, fire protection, employee and visitor security, access and video systems, all aspects of emergency management, and finally training and reallocation of all current personnel resources.

During this assessment the ACCD communications center was a central area of review. The control center acts as the command post and command center for the on-duty incident commander and or the designated ACCD leadership during all emergencies at any and all ACCD facilities. During emergencies, this center is responsible for the coordination of all public safety agencies, employees, clients, visitors, and neighboring businesses and residents. Examples of management of these critical incidents includes but is not limited to emergency evacuations, emergency weather sheltering of major events with up to 18,000 persons in attendance, active shooter scenarios, positive alarm sequence (PAS) management, etc.

Outside of the emergency management role, there is the daily mission of the ACCD control center that acts as a focal point for coordination of logistics and communication in supporting all events. This day today business requires management of people, information, and resources.

In the initial assessment of the control centers current operations, there were several significant deficiencies noted. These included not having an integrated software system in place to support their current role dispatching people, a report management system to track incidents, a database analysis and reports to improve efficiency and effectiveness and a mobile applications- geographic mapping system to allow real time on scene information sharing, or emergency notifications. With this in mind, the ACCD has worked with the City of Austin Communications Technology Management Department (CTM) to research, prepare and fund the system requirements detailed here. In this research it was discovered that the software systems utilized by the larger City of Austin public safety agencies such as APD, AFD, and EMS are similar in general purpose, but they are specifically designed to support larger agencies and while appropriate in their current application would not be able to be shared by ACCD due to their larger scope of required maintenance and financial support.

A contemporary system(s) will address the needs and support the roles of the ACCD Security and Safety Division. Once in place, this system shall provide a safer environment in the day to day business of ACCD, as well as enhance the allocation of resources during any incidence of emergency management.

## 1. SCOPE AND CLASSIFICATION

1.1. This specification establishes the minimum requirements for the purchase of a Computer-Aided Dispatch and Report Management System. The specifications include sections on Functional Requirements, Technical Requirements, Maintenance, and Warranty.

1.2. The Computer-Aided Dispatch and Report Management System shall be used for dispatching security personnel, tracking calls and report records management of security activities at the Austin Convention Center Department.

## 2. APPLICABLE SPECIFICATIONS

2.1. Contractor must be able to provide modules under one product line and not multiple product lines.

2.2. The system must allow compliance with the City of Austin standards as it pertains to records retention scheduling.

2.3. Contractor shall provide a Turn-Key system

## 3. FUNCTIONAL REQUIREMENTS

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 3.1 | Functional | Must Have | The CAD/RMS solution shall allow multiple agencies to share a single CAD/RMS system with one license at no additional cost. | Describe how the CAD/RMS solutions' licensing works. | Licensing |
| 3.2 | Functional | Must Have | The CAD/RMS solution shall allow each agency to individually secure their CAD/RMS program | Describe how the CAD/RMS solution is secured by each individual agency | CAD |
| 3.3 | Functional | Must Have | The CAD/RMS solution shall have a system backup in place with failover protocol. | Describe the CAD/RMS solutions CAD/RMS system backup and fail over protocol. | CAD |
| 3.4 | Functional | Must Have | The CAD/RMS solution shall allow the users to have a minimum of three (3) open screens at a time | Describe the minimum number screens a user is able to have open at one time | CAD |
| 3.5 | Functional | Must Have | CAD/RMS system shall allow configurations and screen views to be saved as dispatcher templates. | Describe, in detail, how the CAD/RMS system shall allow configurations and screen views to be saved as dispatcher templates. | CAD |
| 3.6 | Functional | Must Have | The CAD/RMS solution shall auto-generate incident numbers | Describe how the CAD/RMS solution auto-generates incident numbers | CAD |
| 3.7 | Functional | Must Have | The CAD/RMS solution shall allow users to customize fields | Describe how the CAD/RMS solution allows authorized users to customize fields. Describe which fields are available for the user to customize. | CAD |
| 3.8 | Functional | Must Have | The solution shall allow authorized users to edit pre-installed fields. | Describe how an authorized user is able to customize pre-installed fields. | CAD |
| 3.9 | Functional | Must Have | The solution shall allow authorized users to edit incident types. | Describe how an authorized user is able to customize incident types. | CAD |
| 3.10 | Functional | Must Have | The CAD/RMS solution shall allow messaging between officers, supervisors, dispatchers, and whole groups at one time | Describe how the CAD/RMS solution allows authorized users to message back and forth between officers, supervisors, dispatchers, and whole groups at one time | CAD |
| 3.11 | Functional | Expected | The CAD/RMS solution shall display a predefined procedure (SOP) to the user based on a call type | Describe how the CAD/RMS solution is able to display a pre-defined procedure on the screen based on a call type. | CAD |
| 3.12 | Functional | Must Have | The CAD/RMS solution shall allow authorized users the ability to remote into the system to monitor real time incident log | Describe how the CAD/RMS solution allows authorized users the ability to remote into the system to monitor real time incident logs. | CAD |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 3.13 | Functional | Desired | The CAD/RMS solution shall allow authorized users the ability to schedule tasks/reminders. | Describe how the CAD/RMS solution allows authorized users to schedule tasks/reminders. | CAD |
| 3.14 | Functional | Desired | The CAD/RMS solution shall alert personnel of tasks. | Describe how the solution alerts personnel of tasks/reminders. | CAD |
| 3.15 | Functional | Must Have | In the event of network connectivity failure, The CAD/RMS solution shall, at the least, be able to operate with basic functionality | Describe the CAD/RMS solution's contingency plan when network connectivity is down. What function(s) does the client(s) have? | CAD |
| 3.16 | Functional | Must Have | The CAD/RMS solution shall auto-populate multiple officers as a group | Describe how the CAD/RMS solution auto-populates multiple officers as a group. | CAD |
| 3.17 | Functional | Desired | The CAD/RMS solution shall auto-fill a list of personnel | Describe how the CAD/RMS solution auto-fills a list of personnel | CAD |
| 3.18 | Functional | Must Have | The CAD/RMS solution shall allow officers to self-assign calls | Describe how the CAD/RMS solution allows officers to self-assign calls | CAD |
| 3.19 | Functional | Must Have | The CAD/RMS solution shall allow authorized users to prioritize calls | Describe how the CAD/RMS solution allows authorized users to prioritize calls | CAD |
| 3.20 | Functional | Must Have | The CAD/RMS solution shall utilize drag and drop functionality for call creation and status changes | Describe how the CAD/RMS solution utilizes the drag and drop functionality for call creation and status changes | CAD |
| 3.21 | Functional | Must Have | The CAD/RMS solution shall utilize one-click functionality for call creation and status changes | Describe how the CAD/RMS solution utilizes one-click functionality for call creation and status changes | CAD |
| 3.22 | Functional | Must Have | The CAD/RMS solution's auto-alerts shall be customizable | Describe how the CAD/RMS solution utilizes customizable auto-alerts | CAD |
| 3.23 | Functional | Must Have | The CAD/RMS solution shall have the ability to apply caution flags to person | Describe how the CAD/RMS solution applies caution flags to persons data | CAD |
| 3.24 | Functional | Must Have | The CAD/RMS solution shall have the ability to apply caution flags to locations | Describe how the CAD/RMS solution applies caution flags to locations | CAD |
| 3.25 | Functional | Must Have | The CAD/RMS solution shall allow authorized users to search the CAD/RMS database for vehicle/owner information. | Describe how the CAD/RMS solution allows authorized users to search the CAD/RMS database for vehicle/owner information. | CAD |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 3.26 | Functional | Must Have | The CAD/RMS solution shall specify mandatory completion fields | Describe how the CAD/RMS solution specifies mandatory completion fields | CAD |
| 3.27 | Functional | Must Have | The CAD/RMS solution shall allow the fields to be auto-filled. | Describe what fields in the CAD/RMS solution are able to be auto-filled. | CAD |
| 3.28 | Functional | Must Have | The CAD/RMS solution shall allow authorized personnel to audit all messages | Describe how the CAD/RMS solution allows authorized users to audit all messages. | CAD |
| 3.29 | Functional | Must Have | The CAD/RMS solution shall allow authorized users to view audit trail for report editing. | Describe how the CAD/RMS solution allows authorized users the ability to view report edits | RMS |
| 3.30 | Functional | Must Have | The CAD/RMS solution shall allow authorized users to view audit trail for report viewing. | Describe how the CAD/RMS solution allows authorized users the ability to view report history | RMS |
| 3.31 | Functional | Must Have | The RMS portion of the CAD/RMS solution shall auto-populate with CAD information. | Describe how the RMS portion of the CAD/RMS solution auto-populates with CAD information | RMS |
| 3.32 | Functional | Must Have | The CAD/RMS solution shall automatically route reports via email or text or both. | Describe how the CAD/RMS solution automatically routes reports via email or text, or both | RMS |
| 3.33 | Functional | Must Have | The CAD/RMS solution shall allow authorized users to search the CAD/RMS database for property records. | Describe how the CAD/RMS solution allows authorized users to search the CAD/RMS database for property records. | RMS |
| 3.34 | Functional | Expected | The CAD/RMS solution shall allow for vertical building layering diagrams | Describe how the CAD/RMS solution allows for vertical building layering diagrams. | Other |
| 3.35 | Functional | Expected | The CAD/RMS solution shall integrate with an Emergency Notification System | Describe how the CAD/RMS solution shall integrate with an Emergency Notification system | Other |
| 3.36 | Functional | Must Have | The CAD/RMS solution shall allow a minimum of eight (8) users | Describe the maximum number of users the CAD/RMS solution shall allow. | Licensing |
| 3.37 | Functional | Must Have | The CAD/RMS solution shall support 2 consoles. One (1) Primary dispatch console and one (1) alternate location for back-up and training | Describe the maximum number of supported consoles. | Hardware |
| 3.38 | Functional | Desired | The CAD/RMS solution shall integrate with the Motorola radio | Describe how the CAD/RMS solution integrates with Motorola radio | Hardware |
| 3.39 | Functional | Desired | The CAD/RMS Incident report shall be turned into a 3-1-1 report and sent to 3-1-1 | Describe how the CAD/RMS solution shall turn the Incident report into a 3-1-1 report and send it to 3-1-1 | Other |
| 3.40 | Functional | Must Have | The CAD/RMS solution shall be NDEX compliant | Describe if the CAD/RMS solution is NDEX compliant. | Software |

## 4. TECHNICAL REQUIREMENTS

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.1 | Technical | Expected | The desktop component of the solution should be able to run on the MS XP Operating System (City desktops are managed via the network). In addition, the vendor should have plans to support Microsoft Windows 7 desktop OS. | Describe what operating environment is used by the solution. Indicate whether Microsoft Windows 7 is (or shall be) supported, and when. | Technical |
| 4.2 | Technical | Expected | If the solution is client-server architecture, the client software should be Citrix compliant. | Describe how users can be operated by remote access over a network via Citrix sessions. Indicate whether the proposed solution is currently running successfully in a Citrix environment at customer sites. | Technical |
| 4.3 | Technical | Expected | The vendor must identify any third-party software products used within the proposed system configuration. | List any third-party software products used within the proposed configuration. Include third-party DB management products, report/query tools, client-side products required. Also list any third-party tools supported, but not provided (I.e. report writing | Technical |
| 4.4 | Technical | Expected | Patch updates to operating system software, application software, database software and client software should be tested and identified for implementation within 5 days of a new patch release. | Describe how patch updates are tested and approved for implementation within 5 days of a new patch release (i.e. server, OS, application, browser, and database). Provide the average time required by your organization to test and approve patches and upgrade | Technical |
| 4.5 | Technical | Must Have | The Vendor should provide documentation depicting the technical architecture of the components of this solution, including a simple network architecture diagram. | Provide the documentation of the solution and indicate its limitations. Provide a simple diagram of the proposed solution architecture, showing the hardware components and indicating the types of data exchange between components. | Technical |
| 4.6 | Technical | Expected | The proposed solution client software should not depend on Microsoft Office applications for proper operation. | List any dependencies that the proposed solution has on Microsoft Office applications. | Technical |
| 4.7 | Technical | Expected | If the application is web-based, the solution must support updated versions of Internet Explorer and Firefox client web browsers within 30 days of new releases of the browsers. | Explain how the proposed solution tested and certified for compliance with new releases of Internet Explorer and Firefox web browsers. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.8 | Technical | Must Have | The proposed solution's client interface (whether client software or web browser) must maintain compatibility with routinely updated desktop components such as browser interim update releases, updates to Java and Javascript, Windows OS security patches, e | Describe how your software developers routinely test the application user interface for compatibility with routinely update desktop OS components. | Technical |
| 4.9 | Technical | Expected | The solution should support multiple instances of production, testing (application updates and OS updates) and training environments simultaneously. | Describe how the City can test and validate new releases or updates to the application software and/or operating system prior to putting the updated software into production. Explain licensing requirements for multiple environments. | Technical |
| 4.10 | Technical | Expected | If data archiving is provided, the solution should enable data storage and retrieval from archived data in a manner which is consistent with production integrity. Data Archiving mechanisms must include configuration and metadata elements as part of their | Describe how the application is restored from a backup, and the user environment and the data environment are reestablished, verified, and confirmed. What are ALL the steps required? | Technical |
| 4.11 | Technical | Expected | If data archiving is provided, the solution should allow a user with appropriate privileges to define datasets to be archived, retention periods for current and archived data, and the date and time of archival. | Describe the solution's data archiving solution. Indicate if a user with appropriate privileges can define datasets to be archived, retention periods for current and archived data, and the date and time of archival. Describe all other user-definable featu | Technical |
| 4.12 | Technical | Expected | The solution should allow users with appropriate permissions to view & print application error logs online. | Describe how a user with appropriate permissions views and prints application error logs. Describe the error logs available, and the content of each log. | Technical |
| 4.13 | Technical | Expected | Application updates and operating system security patches should be administered without downtime. | Describe the process used to apply application updates. Describe how the operating system security patches can be administered without downtime. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.14 | Technical | Must Have | The proposed solution must be capable of providing 99.9% uptime if the City of Austin chooses to require it. This level of availability may be directly supported by the proposed solution, or may use third-party tools and methods to achieve 99.9% uptime. | Explain how the solution can be designed to support this level of uptime. Indicate tools and methods supported by the solution to provide the uptime requirement (such as hardware fault tolerance, clustering, mirroring, high availability platforms, etc.). | Technical |
| 4.15 | Technical | Expected | The solution should be able to recover specific data records and/or files from backup and/or near-line storage. | Explain how certain selected records and/or files can be recovered from backup data and made available to the application. | Technical |
| 4.16 | Technical | Expected | The solution should be scalable for future growth. | Provide the number of concurrent users the proposed system can support, and explain the software and hardware changes required to allow growth. Include the licensing structure and the cost levels. | Technical |
| 4.17 | Technical | Expected | Authorized users should be able to control and correct suspended or aborted transactions caused by an unexpected system, network or workstation outage. | Describe how the application administrator can correct suspended or interrupted transactions (i.e. ACID Test Compliance). | Technical |
| 4.18 | Technical | Expected | The solution should include a method of purging record data from the production database(s). | Describe the methods/rules available for purging record data from the production database(s). Explain how referential integrity is enforced when records are purged. | Technical |
| 4.19 | Technical | Expected | The Vendor should explain the relationships between data stored on the main servers, the report servers (if applicable), the training servers (if applicable), the archive servers (if applicable), and any off line data. | Describe the relationships between data stored on the main servers, the report servers, the training servers, the archive servers, and any off line data. | Technical |
| 4.20 | Technical | Expected | The application should manage concurrent data updates by multiple users without creating deadlocks or data loss. | Describe the methods or technologies used by the solution to prevent data loss or deadlock conditions when multiple users are updating data. | Technical |
| 4.21 | Technical | Expected | The solution should ensure master file records cannot be deleted if any child records exist (referential integrity). | Explain how the master file records cannot be deleted if any child records exist. | Technical |
| 4.22 | Technical | Desired | The proposed system should provide data integrity to ensure the accuracy and availability of the data at all times. | Explain how the application ensures data availability and accuracy at all times. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.23 | Technical | Expected | The solution should provide a method for archiving historical data. | Explain the process for archiving historical data. Include information on archiving, retrieval, and purging record data and attached documents. Describe features available to authorized users for selecting records for archiving. | Technical |
| 4.24 | Technical | Desired | If specified in Functional Requirements, the solution should allow one or more files to be attached to, or associated with, a data record. (i.e. text files, scanned images, digital photos, faxes, etc.). | Describe how the solution allows one or more files to be attached to a data record. (i.e. text files, scanned images, digital photos, faxes, etc.) and list the maximum file sizes allowed. Describe how attached files are stored and how they are related to | Technical |
| 4.25 | Technical | Expected | The solution should perform forms-based data validation (field level validation) and display error messages when validation fails (i.e. user enters text in a numeric field). | Explain how the solution validates data entry and handles error messages and the level of criticality of each type of error (i.e. data validation, omitting a required field, etc.). | Technical |
| 4.26 | Technical | Expected | Tables or logs of transaction updates should be maintained that indicate the data element value(s) changed and the date, time, and User ID of the person making the change. | Describe how the solution uses tables or logs of transaction updates to indicate the data elements changed and the date, time, and User ID of the person making the change. | Technical |
| 4.27 | Technical | Expected | If bulk or batch data loads are supported, the solution should use the same data validation criteria for bulk data loads as it does for manual data entry. | If bulk or batch data entry is supported, explain the data validation performed by the application on the bulk loaded data. | Technical |
| 4.28 | Technical | Expected | The application should support user-defined fields, and Application authorized users should be able to create, store, and retrieve data elements that are not part of the standard application. | List any existing user-defined fields and describe the process to add additional user-defined fields. Also describe the process to integrate the user-defined fields in screens, reports, and queries. State any limitations of using user-defined fields. | Technical |
| 4.29 | Technical | Expected | The solution database should be well-documented, including a current data dictionary and Entity Relationship Diagram. | Provide a data dictionary and Entity Relationship Diagram (ERD) for the proposed solution with proposal. | Technical |
| 4.30 | Technical | Expected | Future releases of the application should NOT render archived data unusable. | Describe how historically archived data is supported regardless of changes to the application data schema. | Technical |
| 4.31 | Technical | Expected | The solution should include a transaction update confirmation or failure notification for user transactions, batch transactions and system administrator transactions. | Describe how the application informs the end user of success or failure of attempted transactions, including user transactions, batch transactions and system administrator transactions. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.32 | Technical | Expected | The solution must support DFS shares for file access. | Describe the solution's support for DFS shares. | Technical |
| 4.33 | Technical | Expected | If applicable, all supplied portable devices (laptops, hand-held units, etc.) must have display screens that are readable in conditions ranging from darkness to direct sunlight. | Provide specifications for the included portable device screens (resolution, brightness, backlight, etc.). If possible, provide an evaluation unit. | Technical |
| 4.34 | Technical | Expected | If applicable, all supplied portable devices (laptops, hand-held units, etc.) should be resistant to heat, cold, moisture, dust, and shock. | Provide specifications for provided portable devices in relation to heat, cold, moisture, dust, and shock resistance. | Technical |
| 4.35 | Technical | Expected | If applicable, all supplied portable devices (laptops, hand-held units, etc.) should be capable of receiving program or firmware updates via network connections. | Explain how portable devices can be updated with new program or firmware code changes. | Technical |
| 4.36 | Technical | Must Have | The proposed solution should include a detailed explanation of any real-time or near real-time data interchange required to/from other systems. | List and describe any/all real-time or near real-time data interchange to/from other systems required by the proposed solution. | Technical |
| 4.37 | Technical | Desired | If email is used within the application, the email component should be SMTP and/or Microsoft Exchange compliant and provide a messaging development environment through the provision of documented APIs. | Describe the application's messaging architecture, and indicate if the solution is SMTP and/or Microsoft Exchange compliant and how it provides a development environment through the provision of APIs. | Technical |
| 4.38 | Technical | Desired | The solution must support the import/export of data from/to various other data sources/repositories (i.e. comma delimited, text, HTML, XML, SQL, etc.). | List the various data sources and data formats that the system imports/exports. | Technical |
| 4.39 | Technical | Desired | The solution should generate reports in a variety of file formats, including XML, PDF etc. | Describe the solution's process for generating reports and data extracts files in a PDF format. List all formats allowed by your application. | Technical |
| 4.40 | Technical | Expected | The solution should use standard (published) API's for interfaces to other systems. | List the standard (published) API's that the solution uses to interface with other systems. List any proprietary APIs used. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.41 | Technical | Expected | If the proposed solution requires access to GIS data or an interface to the City's GIS system, the Vendor should specify all spatial software components required, with version(s) supported. | If applicable, list spatial software components required to enable access to GIS data or interface with GIS system. List brands of required software components, along with supported versions. | Technical |
| 4.42 | Technical | Expected | If the proposed solution requires proprietary spatial data to function, the Vendor should specify all required spatial datasets necessary for the solution to operate. | If applicable, list spatial datasets required for the solution to function. List any additional licensing agreements necessary to execute the solution. | Technical |
| 4.43 | Technical | Desired | Reports provided by the application should be compatible with Crystal Reports, or provide a mechanism by which they can be initiated via integration with a Crystal Report's Server. | Describe how the system's reports are compatible with Crystal Reports. | Technical |
| 4.44 | Technical | Expected | If the proposed solution is to be provided to remote end users, the distribution of data should minimize the amount of data sent over the WAN. | Describe the types and volumes of data sent between clients, and clients & servers. | Technical |
| 4.45 | Technical | Expected | The proposed solution's components should be capable of being monitored by network management tools to determine that the components are communicating properly. | Describe how the solution allows the system or network administrator to monitor the solution's availability. | Technical |
| 4.46 | Technical | Expected | The Vendor should use standard Domain Name Services (DNS) for identifying all server components in the system. | Explain how that the system uses standard Domain Name Services (DNS) for identifying all server components in the system. | Technical |
| 4.47 | Technical | Must Have | The solution software must use an accurate, verifiable time source such as GPS clock, NTP or Stratum time source for a traceable time stamp, which is applied to various transactions or key events. | Explain how the solution takes advantage of a traceable time stamp using an NTP source. | Technical |
| 4.48 | Technical | Must Have | If the solution back-end components use date/time stamping, the client-side components should be synchronized with the back-end servers. | Indicate whether the application client components are synchronized with the back-end components, and explain how the sync occurs. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.49 | Technical | Expected | TCP/IP switched and routed protocol must be used as the sole network protocol for both LANs and WANs. | Describe how the systems uses TCP/IP common transmission and management protocol as the sole network protocol for both LANs and WANs. Identify any non-TCP/IP protocols used in the solution (i.e. SMB, NETBEUI) | Technical |
| 4.50 | Technical | Expected | The Vendor should provide a backup process that does not impact the performance of the core system or the availability of online data. | Describe a backup process that does not impact the performance of the core system or the availability of online data. If the proposed solution does not include a backup tool, recommend one that has been tested with your system. | Technical |
| 4.51 | Technical | Must Have | The application must be able to fully support the number of concurrent users specified in functional requirements without any system modification to the application as proposed. | Describe the application limitations for concurrent use. Describe system requirements for growth beyond the specified number of concurrent users. | Technical |
| 4.52 | Technical | Expected | The solution shall not require operating system administrator privileges on the client workstation(s) to run or receive application updates. | Describe the level of privileges required to install application updates and indicate if the application requires workstation administrator privileges to execute or update. | Technical |
| 4.53 | Technical | Expected | If bulk data loads via the Internet are supported by the solution, a secure network transport method for bulk data shall be supported. | Describe how the solution supports secured and/or encrypted transports of data if bulk data load is supported via the Internet. | Technical |
| 4.54 | Technical | Expected | When new users are created, the security permissions assigned to the new accounts shall default to least privileged. | Describe the process of creating a new user in the system, and explain the default system privileges assigned to new user accounts. | Technical |
| 4.55 | Technical | Desired | Authorized users shall have the ability to monitor (in near real-time) and report on file access activities for a particular user, group, application, device, and file. | Describe how the solution provides real-time capability to selectively monitor and report on file access activities for a particular user, group, application, device, and file. | Technical |
| 4.56 | Technical | Desired | The solution shall provide authorized users the ability to track and log all transactions originating from external network sources. | Describe how authorized users track and log all transactions originating from external network sources. Verify that log data includes destination host IP address, originating source host IP address, date, and time. | Technical |
| 4.57 | Technical | Desired | The solution shall display a configurable security banner upon login. | Describe how the solution displays a configurable security banner upon login. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.58 | Technical | Desired | The solution shall NOT use Active Server Pages for web-based communications. | Explain if the solution uses Active Server Pages. | Technical |
| 4.59 | Technical | Expected | To maintain network security, the solution shall include re-assignable ports for the solution. | Provide a list of re-assignable ports utilized by the solution. | Technical |
| 4.60 | Technical | Expected | The solution shall minimize the number of different IP ports and protocols to limit exposure and simplify security administration. | Describe how the solution minimizes the number of IP ports and protocols used and provide a list of IP ports and protocols utilized. | Technical |
| 4.61 | Technical | Expected | The solution shall allow built-in accounts to be renamed. | Describe how built-in accounts can be renamed. | Technical |
| 4.62 | Technical | Expected | The solution shall allow passwords for built-in accounts to be changed. | Describe how built-in accounts can be changed. | Technical |
| 4.63 | Technical | Must Have | When the vendor is connected to the City's VPN for solution support purposes, single tunneling is required (which means that they are disconnected from their local network during the VPN session). | Describe how solution support personnel use VPNs to support the application at the City of Austin site, and indicate whether single-tunneling shall be enforced. | Technical |
| 4.64 | Technical | Must Have | If the solution provides a Web server, the solution's Web interface must be able to operate a secure communication session as SSL 128 bit encrypted HTTPS. | Describe how the solution's Web interface is able to operate a secure communication session as SSL 128 bit HTTPS. | Technical |
| 4.65 | Technical | Must Have | The solution must provide and enforce complex password formats. Passwords must be a minimum of 8 characters, and must allow use of upper and lower case and numeric and special characters. | Explain all password format options provided by the solution, and how passwords are managed and enforced. | Technical |
| 4.66 | Technical | Must Have | Passwords must not be displayed as readable text when users are entering them on-screen. | Describe how system allows end users to type in their password in a non-printing, non-displaying manner (i.e. *****). | Technical |
| 4.67 | Technical | Must Have | Passwords must NOT be included in automated sign-on procedures, stored unencrypted in cache, or transmitted as clear text over the network. | Explain how passwords are managed, stored and transmitted over the network. | Technical |
| 4.68 | Technical | Must Have | The solution must be capable of supporting tiered user permissions to provide application security. | Explain/Describe the tiered permission capabilities the solution offers. Explain how roles/groups/permissions are defined and assigned. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.69 | Technical | Expected | If secure data transport is required, the solution shall provide a method of encrypting the application data between the front-end user system and the back-end servers. | Describe the encryption methodologies provided by the solution for transport of application data. | Technical |
| 4.70 | Technical | Expected | The system shall protect against unauthorized access to data by persons and other software programs. | Describe how system provides security protection against unauthorized access to the database. | Technical |
| 4.71 | Technical | Expected | To help enforce City of Austin's security policies, the solution shall provide a secondary means of identifying system users (i.e. workstation identification numbers, TCP/IP addresses, vendor assigned client IDs, or public key authentication). | Describe how the solution identifies a system user by means other than the user login and password. | Technical |
| 4.72 | Technical | Expected | The application shall provide a transaction log related to changes made to security (roles/groups/permissions). | Provide an example of the security transaction log provide by the application and explain how authorized users can access the log. | Technical |
| 4.73 | Technical | Expected | To help enforce City of Austin's security policies, the solution shall allow the application administrator to disconnect a particular user and to lock out a user during an active session. | Describe how the solution allows the application administrator to lock out a particular user and to disconnect a user during an active session. | Technical |
| 4.74 | Technical | Expected | Authorized users shall be able to define the number of login attempts allowed before a user account is locked and/or disabled. | Describe how authorized users define the number of login attempts before a user account is locked and/or disabled. | Technical |
| 4.75 | Technical | Expected | The solution shall log an event and alert the application administrator when a user exceeds login attempts. | Describe how the solution logs an event and alerts the application administrator when a user exceeds login attempts. | Technical |
| 4.76 | Technical | Expected | The system must automatically log-off a user's work session due to inactivity within a City of Austin-defined period. | Explain the process used to define an inactivity time-out period, and describe what happens when the application detects an inactivity time-out. | Technical |
| 4.77 | Technical | Desired | Authorized users shall be able to create user IDs with an expiration date and time (I.e. for contractors and temps). | Describe how authorized users create user IDs with an expiration date and time. | Technical |
| 4.78 | Technical | Expected | System authorized users shall be able to create security profiles/templates to establish individual and group privileges. | Describe how authorized users create security profiles to establish individual and group privileges. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.79 | Technical | Expected | The application shall allow the Application Administrator the ability to create user groups based on defined roles. | Describe how the Application Administrator can create user groups based on defined roles. | Technical |
| 4.80 | Technical | Expected | The application shall allow the Application Administrator to restrict generic logins. | Describe how the Application Administrator can restrict generic logins. | Technical |
| 4.81 | Technical | Expected | The solution shall allow for the operator to quickly lock the workstation/tablet in the event that they must leave the workstation unattended. | Describe how the solution allows for the operator to quickly lock the workstation/tablet. Explain whether this functionality is provided by the application software or the operating system. | Technical |
| 4.82 | Technical | Expected | The application shall allow the Application Administrator to set the number of concurrent logins for a particular user on the same or on multiple workstations. The application shall generate an alert if a user attempts or exceeds this number. | Describe the methods to limit the number of concurrent logins for a user on the same or on multiple workstations. What are the alerting methods if this number is exceeded? | Technical |
| 4.83 | Technical | Must Have | The solution must allow for multiple security roles for users (i.e.: Admin, Supervisor, Staff etc.) with appropriate permissions. | Describe how the solution functions in relation to user roles. Describe any predefined roles and the system access that each role has. Discuss both application software and DB management user permissions. | Technical |
| 4.84 | Technical | Must Have | If the solution provides the means of user authentication, it must provide the ability for system users to change their active or expired passwords. | Describe how end users can change their passwords, both current and expired. | Technical |
| 4.85 | Technical | Expected | The solution should implement intelligent input entry controls (i.e. drop-down selection lists, pre-formatted screens, shortcut keys, etc.) to make data entry more efficient. | List all intelligent input entry controls used by the solution (i.e. drop-down selection lists, pre-formatted screens, shortcut keys, etc.). If macros or shortcut keys are available, indicate whether they are user-definable. | Technical |
| 4.86 | Technical | Expected | The application data entry forms should retain previously entered data if users must navigate between related screens and/or modules. | Explain how your application retains data when data entry is suspended or interrupted by the user navigating away from the current focus. | Technical |
| 4.87 | Technical | Expected | City of Austin's system authorized users should be able to create and/or modify the content of on-screen error messages. | Describe how authorized users can create and customize error messages displayed to users. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.88 | Technical | Expected | End users should not have to log in separately to different modules of the application. A single sign-on should be all that is required. | Describe how system allows a user to sign on once to access the entire application according to their access rights. | Technical |
| 4.89 | Technical | Expected | If the application provides help messages and/or usage tips, such screen messages should be definable by the City of Austin's application administrator(s). | Provide screen shots of help screens and usage tip displays available to the application user. Explain how application users with appropriate permissions can define the text of help and tip messages. | Technical |
| 4.90 | Technical | Expected | The solution should include functionality for cut, copy, paste, and undo. | Describe how the solution includes functionality for cut, copy, paste, and undo. | Technical |
| 4.91 | Technical | Expected | The solution should reduce repetitive keying for data entry fields such as dates, city, state, zip, etc. | Explain how the solution reduces repetitive data entry in application forms and/or tables (i.e. pre-fills, look-ups, etc.). | Technical |
| 4.92 | Technical | Expected | A customizable application user interface should not require modification of program code. | Indicate how user screens and other user interface components may be customized by the City of Austin without requiring modification of program code. | Technical |
| 4.93 | Technical | Expected | A customizable application interface should not prevent the application from benefiting from future updates of the software. If the application is customized, there is assurance that future upgrades and bug fixes shall work without additional fees, time or | Describe how the user interface may be customized by the City without affecting future updates and bug fixes. | Technical |
| 4.94 | Technical | Expected | The solution should support automated alerting of specified users when key components are unavailable (such as DBMS, servers, interfaces, network transport). | Describe the solution's tools/methods that support alerting of specified users when key resources are unavailable. | Technical |
| 4.95 | Technical | Must Have | If the solution uses Oracle, it must use minimum release level of version 10g. | For Oracle databases, describe what version of Oracle the database supports and if 9i can be updated to 10g. | Technical |
| 4.96 | Technical | Expected | The solution should be capable of utilizing computer storage devices (SAN). | Describe how the solution supports a SAN storage solution. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.97 | Technical | Expected | The solution should allow real-time monitoring, logging, and reporting on key application performance metrics, and should allow for the coexistence of non-invasive Database performance monitoring tools like Oracle Grid control and/or Idera Software. | Explain the method(s) provided with the application (if any) that provide real-time monitoring, logging and reporting on specific application performance metrics. If no monitoring is provided with the application, recommend a monitoring solution supported | Technical |
| 4.98 | Technical | Must Have | Executable server software processes must be capable of running as service(s) (or daemon(s)) that run automatically upon system start-up, and do not require a user login to start up. | Explain how server-side software processes are executed automatically, and indicate whether the processes are designed to be service (or daemon) processes. | Technical |
| 4.99 | Technical | Expected | The Vendor should specify any requirements for job scheduling software. The City currently supports UNIX CRON, Tivoli Work Scheduler, Oracle DBMS_JOBS and MS SQL DTS. | List any software requirements for job scheduling and explain what software is required, and what jobs are run via the scheduler. | Technical |
| 4.100 | Technical | Desired | The City prefers Linux/UNIX OS for public web servers. Windows 2003 and 2008 Server and Linux/UNIX operating systems are acceptable for internal servers. | List the operating systems on which each component of your application shall run. If choices exist, indicate the OS's most commonly used by existing clients. | Technical |
| 4.101 | Technical | Desired | Linux/UNIX or Windows operating systems are preferred for application servers. | List the operating systems on which each component of your application shall run. If choices exist, indicate the OS's most commonly used by existing clients. | Technical |
| 4.102 | Technical | Expected | If applicable, the solution should be implemented using N-tier architecture. N-tier implementation should be capable of supporting load balancing across a series of solution servers. | Explain how the solution is implemented within the N-tier architecture, including load balancing across a series of solution servers. | Technical |
| 4.103 | Technical | Expected | The Vendor must propose both minimum and optimal specifications for the servers (if applicable), client workstations, and mobile computing devices. This equipment must have the capacity to do run the proposed application, perform data analysis, querying a | List the minimum AND optimal recommended specifications for servers (if applicable), client workstations, and/or mobile devices to run the application. Include estimates for server and database storage requirements based on similarly sized municipalities. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.104 | Technical | Must Have | If the proposed solution requires an Application Server, specify the recommended platform, including Operating System, OS version(s) and OS release(s) supported. | If applicable, provide both recommended and optimal specifications for the Application Server(s), along with Operating System, OS version(s) and OS release(s) supported. | Technical |
| 4.105 | Technical | Expected | The City of Austin should be able to accurately plan for storage and backup requirements, both for initial implementation and for future growth. | Provide capacity estimates (in terms of GB of storage) for the proposed system on-line storage and data archives. | Technical |
| 4.106 | Technical | Expected | The solution should be supported in a virtual server environment based on VMWare Infrastructure 3. | Describe your support for running the application software on VMWare or other virtual server environments. | Technical |
| 4.107 | Technical | Must Have | The proposed solution must be capable of being fully restored in the event of catastrophic server failures. | Describe the data and application backup and recovery plan including automatic and unattended backups, expected data loss from recovery, backups in a separate facility from the production system, and allowances for full or partial recovery. | Technical |
| 4.108 | Technical | Desired | If the proposed solution includes fail-over, the fail-over event should be completely automated. | Describe how the system performs automatic fail-over between redundant systems in the event of system failure for both the application and the database. | Technical |
| 4.109 | Technical | Expected | The RDBMS used by the solution (if applicable) should support transaction logs and allow a data restore from transaction logs. | Explain how the solution's RDBMS supports transaction logs and allows for a data restore from those logs. | Technical |
| 4.110 | Technical | Expected | The system should include a backup and recovery plan for data, data structures, application software files, executables, and application software utilities. The plan should include a backup and recovery test plan. | Describe the backup and recovery plan. It should address automatic and unattended backups, expected data loss, backups in a separate facility from the production system, emergency notification procedures, and procedures for full or partial recovery. | Technical |
| 4.111 | Technical | Expected | If the solution uses relational database management technology, it should be capable of supporting high availability and resiliency. | Describe how the solution RDBMS can provide availability and resiliency through the use of such technologies as mirror imaging, portability, and replication. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.112 | Technical | Expected | The software environment should be capable of dynamically accepting changes to network configurations with little or no impact on solution availability (i.e. Installing additional servers/workstations and changing the IP or subnet of any of the servers). | Describe how the solution is capable of dynamically accepting changes to network configurations with no impact on solution availability (i.e. Changing the IP or subnet of any of the servers should not affect operation). | Technical |
| 4.113 | Technical | Must Have | If the proposed solution provides high availability (HA) level of service, specify the HA components required (such as Oracle RAC or Data Guard), and indicate if such components are included in the proposal. | List the HA components (if applicable) required, and specify whether the components are included in the proposal or are to be provided by the City. | Technical |
| 4.114 | Technical | Must Have | If the application software is designed for mobile communications, the application software must provide features that protect against data loss when roaming between different networks. | Describe how the application software provides features that protect against data loss when roaming between different networks. | Technical |
| 4.115 | Technical | Must Have | The solution should use a widely accepted and well-supported DBMS such as Oracle 10g (or higher) or MS SQL 2000 SP3. | Describe the database system(s) and version numbers supported by the solution. (Oracle systems with processor-level licensing are preferred but MS SQL is accepted.) | Technical |
| 4.116 | Technical | Expected | The Vendor should provide recommendations for tuning parameters for all databases. | Provide recommendations for tuning parameters for all databases. Explain the reasoning for these recommendations. | Technical |
| 4.117 | Technical | Expected | If the proposed solution uses an RDBMS system other than Oracle 10g (or higher) or MS SQL 2000 SP3 (or higher), the RDBMS should support two-phase commit procedures. | Explain how the RDBMS used by the solution supports two-phase commit procedures. | Technical |
| 4.118 | Technical | Expected | If the proposed solution includes a relational database management system other than Oracle or MS SQL, the RDBMS must be ACID compliant. | Provide evidence that the proposed RDBMS is ACID compliant. | Technical |
| 4.119 | Technical | Expected | The proposed solution should support Service Oriented Architecture. | Describe how the proposed system supports SOA, and specify what SOA services and platforms are supported. | Technical |
| 4.120 | Technical | Must Have | If the proposed solution uses Oracle DBMS, and is client-server architecture, specify the required number of Oracle client licenses. | Specify the required number of Oracle client licenses, and indicate if the licenses are included in the cost proposal. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.121 | Technical | Expected | The solution should be able to run in a VLAN environment. | Describe how the solution runs in a VLAN environment. Note any limitations of running the solution in a VLAN environment. | Technical |
| 4.122 | Technical | Desired | The system components should be capable of using SNMP (V3) to report system metrics via the network. | Explain how the system uses SNMP V3. Describe which hardware and software components of solution (provided by Vendor) are SNMP V3 capable. | Technical |
| 4.123 | Technical | Must Have | The solution should be able to run in an environment that uses 100/1000MB full duplex connections for back-end systems. | Describe how the solution runs in an environment that uses 100/1000MB full duplex connections for back-end systems. | Technical |
| 4.124 | Technical | Must Have | If the proposed solution includes electronic hardware such as servers or network devices, all network-enabled hardware must support auto-negotiation of network speeds and duplex settings, including 10 mbps, 100 mpbs and Gigabit Ethernet, if applicable. | Provide specifications on network interfaces of all network-enabled devices proposed. | Technical |
| 4.125 | Technical | Must Have | Application servers should NOT require Layer 2 adjacency. | Explain any limitations relating to Layer 2 adjacency requirements for the proposed application. Can all application server components be separated on different network segments or sub networks? | Technical |
| 4.126 | Technical | Must Have | The proposed application should NOT require static network routes. | Explain how inter-network communications are supported in the application without the need for statically assigned routes. | Technical |
| 4.127 | Technical | Expected | The proposed solution should be compatible with, and easily supported on the City of Austin's native network infrastructure. | Provide documentation of application/data traffic including protocols and ports. List the ports and protocols used for data communication between each tier of the application. Note any exceptional aspects of the application communication architecture. | Technical |
| 4.128 | Technical | Must Have | The proposed solution must not require broadcast messaging for normal operation. | If the application must use broadcast messaging, describe the purpose and functionality of broadcasting. | Technical |
| 4.129 | Technical | Expected | The proposed solution must be capable of operating over routed sub networks (does not require components to be co-located on the same sub network). | Explain how the proposed solution components can communicate with each other when separated on different sub networks. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.130 | Technical | Expected | If the proposed system components support SNMP, the Vendor must provide standard MIB files for all SNMP-enabled components. | Provide a list of SNMP MIBs available and supported by the proposed system. | Technical |
| 4.131 | Technical | Expected | The solution should be capable of providing a current copy of the production data that allows system users to perform queries, perform data mining, and produce reports on servers other than the production servers. | Describe the data archiving solution that allows system users to perform queries and produce reports on servers other than the production servers. | Technical |
| 4.132 | Technical | Expected | The solution shall provide RADIUS, LDAP, or MS Active Directory authentication to provide authentication to the application software, and should provide a scheme for Group level definition and implementation within the LDAP services. Additionally, the sof | Describe what authentication methods are supported by the application software. | Technical |
| 4.133 | Technical | Must Have | If the solution includes a firewall, it must not use an application-layer proxy firewall. The solution must use a stateful-inspection firewall instead. | Confirm that the solution does not use an application layer firewall. | Technical |
| 4.134 | Technical | Expected | All Windows-based solutions deployed on both client workstations and servers shall be compatible with Trend Micro Anti-Virus and SMS for servers and workstations. | Describe how the application is tested and validated as being compatible with the Trend Micro Anti-Virus application and SMS. | Technical |
| 4.135 | Technical | Expected | System directories affected by City of Austin-installed system-hardening software must be easily identifiable by Security Administrators so they shall know which directories to lock. | List all directories affected by system-hardening software. If the City installs system-hardening software on the system, Security Administrators need to know which directories to lock. | Technical |
| 4.136 | Technical | Expected | The Vendor should maintain a recovery test plan and recovery test procedures that result in a full recovery of the system following full and partial system failures. | Provide a copy of your recovery test plan and procedures, and provide documentation of periodic tests performed. | Technical |
| 4.137 | Technical | Must Have | There is no acceptable loss of data due to system failure. | Describe how system ensures that no data is lost in case of system failure. Include a discussion of the backup procedures used to meet this requirement. | Technical |

| # | Type | Importance | Requirement | Required Response | Category |
|---|---|---|---|---|---|
| 4.138 | Technical | Must Have | Hosted solutions must provide a method for the City to periodically download and store copies of the hosted data on City-provided storage. | Describe how City of Austin can create and periodically update off-line copies of City of Austin data. Explain the types of connections available to retrieve data, and how data retrieval can be scheduled. | Technical |
| 4.139 | Technical | Must Have | Authorized users must be able to receive a complete copy of current and archived data hosted by an ASP provider in the event of contract termination. | Explain how current and historical data can be received by City of Austin if the contract is terminated for any reason. | Technical |
| 4.140 | Technical | Expected | The application's client should be capable of running over a low-speed connection of as slow as 128kbps. | Describe the minimum client bandwidth required, and the recommended bandwidth. | Technical |
| 4.141 | Technical | Must Have | The vendor must conduct a 3rd party annual security assessment of all tiers of its hosting facility, including application servers and network devices. Copies of the security audit reports must be provided to the City of Austin annually. | Describe how an external audit of the proposed system security will be provided. | Technical |
| 4.142 | Technical | Must Have | All user access must be logged with time-stamped entries, and the log made available to the City of Austin. | Describe what user access logs are kept and made available to City of Austin, and how they are accessed. | Technical |
| 4.143 | Technical | Desired | If, as a result of annual security assessments, high vulnerabilities are discovered, they must be remediated immediately. | Explain how security vulnerabilities will be remediated at the ASP facility | Technical |
| 4.144 | Technical | Expected | All packets passing through the gateway and/or firewall to the application servers must be logged, and logs be kept for a minimum of (10) days. | Explain the network security logging performed and monitored by your hosting facility. | Technical |
| 4.145 | Technical | Expected | Sensitive data is to be protected, the solution must support a form of network session encryption. | Explain the types of session encryption supported. | Technical |
| 4.146 | Technical | Must Have | City of Austin data must not be made available to any other parties not specifically authorized to view or access the data. | Describe how City of Austin data is protected from access by unauthorized parties. | Technical |

## 5. IMPLEMENTATION REQUIREMENTS

### 5.1. Implementation Plan

5.1.1. Provide documentation describing proven project management methods to include:

- Project Management Methodology (Model) Used

- Explanation of the Methodology
- Explanation of how the Methodology shall be used in this project

5.2. **Training**

5.2.1. Contractor shall provide a detailed training plan and training that includes system administrator, technical training, and end user training.
5.2.2. Contractor shall provide training materials that can be adapted for use by City staff to conduct end user training.
5.2.3. The Contractor shall submit with proposal recommendations on how to conduct ongoing training for new users and training for future upgrades.

5.3. **Maintenance**

5.3.1. The Contractor shall respond to all problem requests received from the City once system is in production. An initial response shall be received within one (1) hour, critical problems shall be addressed and resolved within eight (8) hours, with all other production problems addressed and resolved within twenty-four (24) hours.

5.3.2. Provide a plan for support and maintenance for a one year following the warranty period
The plan should include information on how to contact the Vendor, the availability of the Vendor support team, and levels of service and associated response times. In addition, the plan should include information regarding what software/hardware is supported in the maintenance plan, the cost of the plan, information about warranties, and information about enhancements and upgrades

5.4. **Warranty**

5.4.1. Vendor shall propose, in detail, the warranty for covered items