THE CITIES OF KELLER, COLLEYVILLE, SOUTHLAKE, WESTLAKE, AND GRAPEVINE TX

REQUEST FOR PROPOSAL

RFP Number:	20-011
RFP Title:	Multi-City Computer Aided Dispatch, Records Management System, Detention Management System, and Field Mobile RFP

Submittal Deadline	
Date:	March 20, 2020
Time:	2:00 PM CST
Location:	The City of Keller, TX
Address:	**RFP Mailing Address:** City of Keller Purchasing Agent P.O. Box 770 Keller, Texas 76244

RFP Courier Delivery Address: City of Keller Purchasing Agent 1100 Bear Creek Pkwy. Keller, Texas 76248 |

RFP TIMELINE: The **anticipated** schedule for this RFP is as follows:

RFP Issue Date	February 19, 2020
Pre-Proposal Conference Call	March 03, 2020, 1:00–2:00 PM CST
Final Written Questions Due	March 05, 2020, 5:00 PM CST
Responses Addenda Posted	March 11, 2020
Proposal Submission Deadline	March 20, 2020, 2:00 PM CST
Shortlist Notification	April 03, 2020
Onsite Demonstrations	May 19 – 28, 2020
Contract Negotiations	July 2020
Contract Award	August 2020

Table of Contents

This Page Intentionally Left Blank

1.0 INTRODUCTION AND VENDOR INSTRUCTIONS

1.1 Introduction

The Cities of Keller, Colleyville, Southlake, Westlake, and Grapevine TX (referred to as "the Consortium") invite your company to provide a proposal for the implementation of a comprehensive, turnkey, fully-integrated Computer Aided Dispatch and Records Management System with associated Field Based Reporting and Detention Management functionality (CAD/RMS/FBR/DMS). The system may either be locally-hosted or web-based Software as a Service (SaaS) hosted and fully supported by the Vendor. Vendors must propose all the modules of a full system solution.

Services associated with the implementation of the Computer Aided Dispatch and Records Management System would include: project management, system design, hardware, any software customization to meet specifications, interface development, systems integration, data migration, testing, implementation and training.

1.2 Multi-City Public Safety Systems Consortium Background

Five cities in the Dallas-Fort Worth metropolitan area have formed a regional Multi-City Public Safety Systems Consortium. The City of Keller provides police and fire dispatch and detention facilities for themselves and three other cities: Southlake, Colleyville and Westlake. Each individual city manages their own records management. Grapevine, while a part of the consortium for data sharing purposes, manages their own dispatch, records management, and detention facilities and therefore will be separate from an architecture perspective. The Cities provide law enforcement, fire, and rescue services to their municipal residents.
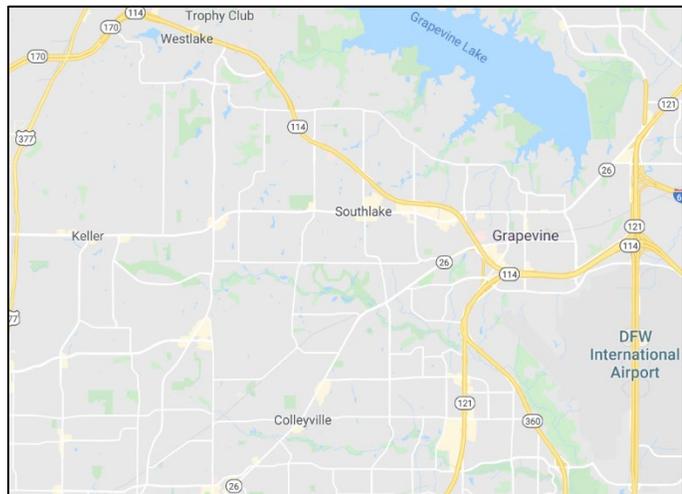
The population estimates for the five Cities, as of the most recent statistics, are:

City	Population
Keller	47,266
Colleyville	26,674
Southlake	31,824
Westlake	1,483
Grapevine	53,982
Total Consortium	**161,229**

The Cities' Communications Centers, Detention Centers, Police, and Fire Departments operate 24 hours a day, 7 days a week, and 365 days a year. From January 2018 to December 2018, there were an estimated 69,583 9-1-1 calls. These break down by City as follows:

City	# of 911 Calls
Keller	15,000
Colleyville	7,000
Southlake	17,183
Westlake	400
Grapevine	30,000
Total Consortium	**69,583**

During this same period, police handled 50,700 dispatched calls-for-service and 11,064 incident reports were written, while fire handled 15,482 calls-for-service.

The Consortium Organization

The mission of the Multi-City Public Safety Systems Consortium is to serve as law enforcement leaders in protecting and assisting all people in our community through effective problem solving, professional service, and clear transparency. The Consortium is comprised of dedicated team members focused on partnering and engaging with our community as we work to make our communities a great place to live, visit and conduct business. Our proactive, engaged and transparent policing model has proven successful in reducing crime and fear of crime in the local area and promotes fair and just treatment to all with whom we come into contact. The Consortium's mission is driven by our E4 core value system, which is the foundation for all that we do:

- Empathy – We actively listen, view perspectives of others and always seek to understand.

- Edification – We work to build relationships in all we do, understanding that all stakeholders play a key role in public safety and quality of life.

- Enthusiasm – Police members have a passion to serve and embrace their role as guardians within their community willing to go above and beyond in a moment's notice to safeguard our community against crime, fear and disorder.

- Excellence – A commitment to continuous improvement personally, professionally and as an organization as we meet the needs of our growing community.

1.3 Project Intent

The Consortium is currently seeking to replace its current CRIMES CAD/RMS systems, including the following modules: Call Taker, Dispatch, CAD Administration, Fire Dispatch, Reports Management, Crime Analysis, Case Management, Civil Process, Mobile Field Based Reporting, and Detention Management.

1.3.1 Project Scope

Proposals are being sought through this RFP for a project that includes acquisition of:

- Call Taker Capabilities (i.e., Event Initiation and Processing, Event Updates, Address Validation, Processing Duplicate Calls for Service, Event Priorities)
- Dispatch Capabilities (i.e., Dispatch Decision Support, BOLO, Dispatch Units, Unit Status Management, Call Management, Supplemental Resources Tracking, Call Disposition)
- Administration Capabilities (i.e., Geofile Maintenance, Security, Logging, Configuration, Table Maintenance, Communication Center Relocation, CAD Catch-Up)
- Reports Management Capabilities (i.e., Report Entry/Edit/Approval, Report Indexing, Database Inquiry, Agency Reporting (NIBRS), Management Reporting, Incident Reporting, Racial Profile Reporting, Payments & Accounts, Productivity Reports)
- Crime Analysis Capabilities (i.e., Statistical Data, Traffic Summary, Arrests, Master Name Index, GIS mapping, Crime Patterns, Criminal History)
- Property and Evidence Capabilities (i.e., Intake, Storage, Barcoding, Digital Files, Status Updates, Notifications, Evidence Management)
- Case Management Capabilities (i.e., Case Initiation, Document Management, Reports Management, Master Name Merging, NIBRS Reporting, Warrants, Electronic Ticketing, Citations, Scheduling and Calendar)
- Detention Management Capabilities (i.e., Intake, Custodial, Administration, Reports)
- Civil Process Capabilities (i.e., Document Generation and Management, Inquiring, Protection Orders, No Contact Orders, Eviction Orders)
- System Integration Services
- Interfaces to certain Consortium systems
- Training
- Maintenance Services.

1.3.2 The Consortium's Preferred Solution

The Consortium will issue a single request for proposal (RFP) for the entire system. The organization will entertain proposals from both integrated system vendors, as well as best-of-breed component proposals. Vendors whose system does not include all components may choose to partner with others to provide a complete solution to member agencies. However, the organization will contract with a single vendor who brings the complete solution to them as the prime integrator; the Consortium will not act as the prime integrator itself.

The Consortium plans to implement an industry standard, commercial-off-the-shelf (COTS) modular software solution. The committee is willing to consider a software-as-a-service solution. The Consortium has standardized on the Microsoft Operating Systems platform and future solutions will operate on Windows 10 desktops, self-hosted options must utilize Windows Server 2016 and higher, and both Android and Apple iOS (iPhones/iPads) mobile environments. Solutions that incorporate Web Services Internet/Intranet technology will also be considered.

It is critical to the success of this project that the vendors perform extensive business analysis and provide process improvement recommendations to take full advantage of the proposed solution's potential. Solutions that are inflexible and require complete changes to our existing processes are unlikely to be selected. A balanced approach that allows for configuration changes to adjust the software to meet our needs is the most likely to succeed.

The Consortium is looking to establish a long-term relationship with a vendor. As such, the Consortium is looking for a vendor whose primary business is the Public Sector and has a proven track record of:

- Financial stability
- Successfully implementing its system with multi-agency groups
- Sustained history of significant re-investment in its software to keep it modern in terms of functionality and platform.

1.3.3 Consortium Objectives

The objectives of this deployment include:

- Would prefer to see a CAD/RMS/FBR/DMS that has a broad functionality for multiple components. It may not be the best in one area but is very functional overall, i.e. best of breed vs. unified system
- Would also like to see a vendor that is innovative and looking to add functionality as technology progresses
- A system that comes highly recommended and has other user groups in the state of Texas.
- It would also be an advantage to go with a company that has an accessible and knowledgeable customer support
- The system should simplify the process for field units when documenting field events, i.e. case reports, archiving photos and evidence
- The system should have a comprehensive and highly effective statistical gathering and analysis function that is user friendly and easily manipulated to suit departmental needs
- Full GIS Integration with real-time updates to create a multi-city regional map
- The ability for the Master Name Index to be developed where it provides the flexibility to perform searches against the database can be drilled down to either a single City or searched against the entire Consortium
- Automate and integrate functions currently requiring manual intervention

- Move to a system that provides a high degree of configurable parameters instead of customization
- Reduce/eliminate redundant data entry
- Provide improved data analysis and reporting through easy for average users to use, customizable reporting tools and modern analytical toolsets
- Have a fully integrated Electronic Document Management System for file scanning, storage, electronic forms processing, and workflow
- Ability to rapidly recover the CAD/RMS/FBR/DMS system from a critical event
- Encourage new process development.

The Consortium requires that a single Vendor propose all project elements, subcontracting certain aspects as necessary. The Consortium has a preference for an integrated set of modules over interfaces. The Consortium requires proposals with the following project elements:

- Business Process Engineering
- Server hardware and software setup to include:
  - Operating System
- Application Software to include:
  - CAD Module
  - RMS Module
  - FBR Module
  - DMS Module
- Software Implementation
- Mapping System Integration
- Data Migration
- Internal and External System Interfaces
- Comprehensive System Training
- Software Maintenance & Support.

Additionally, the Consortium seeks assurance of:

- Effective Project Management by the Vendor and the Vendor's Project Manager within the Vendor's organization
- Long-term useful life of the system
- Vendor's commitment to keeping the system state-of-the-art
- Competitive prices.

The Consortium desires to procure the most appropriate system within its financial means from a qualified vendor at a firm, fixed price. The Consortium prefers to purchase an existing system that is in use by other similar agencies and is proven effective. Contracts shall be made only with a responsible Vendor who possesses the ability to perform successfully under the terms and conditions of this proposed procurement. Consideration shall be given to such matters as software and hardware quality, Vendor integrity, record of past performance including prior successful implementation of proposed products, and financial and technical resources.

Each firm submitting a proposal must have established a state and/or national reputation for the planning, supplying, installing and maintaining of their systems. Firms are required to provide, as part of their normal updates, all changes to federal and state reporting forms and reports as they issued by those agencies.

The Consortium is interested in purchasing the best functional fit that it can afford. Consequently, although the Consortium is requesting proposals for complete systems, including hardware, software, and services that include any and all third-party components, the Consortium may choose not to acquire all system components proposed. The Consortium may also exercise the option to procure third-party components directly using vendor-provided specifications (i.e., servers, field mobility devices).

It is important for the proposers to understand that the Consortium has invested in its infrastructure and expects to leverage that infrastructure. The Vendor is expected to (a) specify hardware and network requirements as part of its proposal, and (b) propose services that enable it to certify that the hardware and network utilized by the Consortium meets its minimum standards so that the Vendor can comply with performance requirements specified in this RFP.

1.4 Key System Functions

Certain key system functions are of particular interest to the Consortium. These will be given a higher weight during the evaluation process and must be shown during the Demonstration phase of the evaluation process.

- Fully integrated Computer Aided Dispatch, Records Management, Field Mobile, and Detention Management functions
- A CAD/RMS/FBR/DMS that has broad functionality allowing for multiple components. It may not be the best in one area but is very functional overall (i.e., unified system preferred over best of breed)
- A system that simplifies the process for field units when documenting field events (i.e., case reports, archiving photos and evidence)
- Single CAD Mobile and FBR application where information flows between the two automatically and allows for a complete RMS search from within the Mobile
- Mobile application is ergonomically designed for field use (i.e., large buttons) and operates in a disconnected mode
- Comprehensive and highly effective statistical gathering and analysis functions that is user friendly and easily manipulated to suit departmental needs
- Fully integrated electronic document management system for file scanning, storage, electronic forms processing, and workflow
- Reduce/eliminate redundant data entry
- Automating manual processes to reduce staff workloads
- High degree of configurable parameters instead of customization
- Provision for improved data analysis and reporting through easy to use, customizable reporting tools and modern analytical toolsets.

1.5   RFP Outline

The following table provides an outline of the RFP.

#	Section	Purpose
1.0	Introduction & Vendor Instructions	This section contains background information, instructions on how to submit a proposal and a guideline for the proposal contents and format.
2.0	Background and Functional Requirements	This section provides an operational background of the agency and a description of the current systems, as well the requirements for new ones.
3.0	Infrastructure Requirements	This section provides the requirements for the technical infrastructure supporting the system, whether Vendor-Hosted or On-Premise, as well as ongoing performance/update requirements.
4.0	Service & Maintenance Requirements	This section contains requirements for ongoing system maintenance and other services over the life of the system(s).
5.0	Acceptance Testing Requirements	This section contains requirements for the initial acceptance of the system.
6.0	Implementation Requirements	This section contains requirements for the conduct and completion of the implementation period.
7.0	Contract Requirements	This section defines the general business relationship to be established with the Vendor.
8.0	Price Requirements	This section describes the pricing details required and the payment and other related terms.
	Attachments	Attached files: ▪ A1 - Proposal Response Forms ▪ A2 - Functional Requirements Response Forms o FRR – General System o FRR – Computer Aided Dispatch System o FRR – Records Management System o FRR – Detention Management System ▪ A3 - Consortium Required Forms ▪ A4 - Consortium Terms and Conditions

1.6   Proposal Process Instructions

1.6.1   Significant Dates

It is intended that the following dates will govern this procurement. They are subject to change at the discretion of the Consortium.

Activity	Date/Time
RFP Issue Date	February 19, 2020
Pre-Proposal Conference Call	March 03, 2020, 1:00–2:00 PM CST
Final Written Questions Due	March 05, 2020, 5:00 PM CST
Reponses Addenda Posted	March 11, 2020
Proposal Submission Deadline	March 20, 2020, 2:00 PM CST
Shortlist Notification	April 03, 2020
Onsite Demonstrations	May 19 – 28, 2020
Contract Negotiations	July 2020
Contract Award	August 2020

1.6.2   Communication with the Consortium

All communications regarding this RFP from Vendors and other sources must be directed to the RFP Coordinator as follows:

Title	Purchasing Agent
Name	Karla Parker
Address	City of Keller 1100 Bear Creek Pkwy. Keller, Texas 76248
Email	kparker@cityofkeller.com

Contact with the Consortium member cities or any of their employees regarding this procurement is expressly prohibited without prior consent of the RFP Coordinator.

1.6.3   Pre-Proposal Conference Call & Questions

The purpose of the Pre-Proposal Conference Call is to provide interested vendors with an opportunity to obtain clarification, from subject matter experts, regarding the specifications and requirements outlined in this RFP.

The Pre-Proposal Conference Call date is listed in Section 1.6.1; this meeting is NOT mandatory. The meeting will be held via audio conference. Instructions for the dial-in to the audio conference can be obtained by sending an email to the RFP Coordinator at the address in Section 1.6.2.

It is preferred that all questions, comments and requests be received via e-mail no later than one (1) business day prior to the conference call. This will allow the RFP Coordinator time to review the questions and prepare responsive information prior to the pre-proposal conference call. Vendors may also ask questions, make comments, or request information during the pre-proposal conference. Verbal questions may be discussed at this conference call. However, all answers provided verbally will not be considered binding. The only official answers will be posted in writing in the form of an RFP Addendum on or before the date listed in Section 1.6.1.

Vendors are encouraged to submit questions or comments, or make requests for information or clarifications until the Final Written Questions Due date identified in Section 1.6.1. All questions must be submitted via email to the address in Section 1.6.2. No additional questions will be responded to after the Written Questions Due date listed in Section 1.6.1.

1.6.4   Proposal Submittal

Vendors must deliver two (2) electronic copies (i.e., flash drive) of the Proposal Response Forms and Functional Requirements Response Forms (spreadsheets) in their native Word and Excel formats on or before the Proposal Submission Deadline identified in Section 1.6.1. Electronic images or .pdf versions of these files will not be accepted as compliant. In addition, Vendors must deliver a hard copy of one (1) original signed copy, six (6) bound copies, and current insurance certificate to the address shown below. Submissions must be signed by the person authorized by your company to commit your company to all instructions, conditions and pricing as defined, or entered in or on, the proposed documents. The proposals containing original signatures must be clearly marked "**ORIGINAL**".

Proposals submitted via email or facsimile will not be accepted. Proposals returned in a non-compliant format may be considered "non-responsive" and can be rejected. For supplemental information, place that information at the end of the section marked: "Vendor Supplemental Information".

All hard copy proposals must be delivered to the address shown below on or before the Proposal Submission Deadline identified in Section 1.6.1. Submit documents in a sealed envelope with the following information marked plainly on the front:

	RFP Mailing Address:	**RFP Courier Delivery Address:**
Address	City of Keller Purchasing Agent P.O. Box 770 Keller, Texas 76244	City of Keller Purchasing Agent 1100 Bear Creek Pkwy. Keller, Texas 76248
Date:	March 20, 2020, 2:00 PM CST	
Title:	ATTN: PURCHASING DEPARTMENT MULTI-CITY COMPUTER AIDED DISPATCH AND RECORDS MANAGEMENT SYSTEM PROPOSAL	
RFP #:	20-011	

In addition, Vendors must conform to the following:

- Vendors must follow the format outlined in Section 1.5 and fill out completely the form(s) furnished in:

  o A1 - Proposal Response Forms;
  o A2 - Functional Requirements Response Forms; and
  o A3 – Consortium Required Forms

- Any costs associated with preparing proposals in response to this RFP are the sole responsibility of the Vendor.
- All proposals and supporting materials as well as correspondence relating to the RFP become the property of the Consortium when received.
  o Any proprietary information contained in the proposal should be so indicated.
- The Vendor is responsible for assuring proposal delivery on or before the stated date and local time as well as for any associated delivery costs. The Consortium is not responsible for lateness for any reason (i.e., mail, carrier). Proposals submitted after that date will not be considered.
- The Consortium reserves the right to refuse all proposals in their entirety or select certain components and/or services from various proposals.
- Any exceptions to the specifications must be stated on the Proposal Response Forms.
- Additional instructions, general terms and conditions are provided in the Attachment A4 - Consortium Terms and Conditions.
- The Consortium reserves its right to reject any or all proposals at any time, with or without cause.

1.7   Definitive List of Proposal Contents

The Consortium requires a uniform proposal format so that all proposals can be fairly evaluated.

1.7.1   Response Format

Vendors are advised that the Consortium's ability to evaluate proposals is dependent on the Vendor's ability and willingness to submit proposals which are well-ordered, detailed, comprehensive, and readable. Clarity of language and adequate, accessible documentation is essential.

Vendors must follow the response format outlined in the table below. In addition, response forms have been provided and must be used to allow each Vendor to provide a uniform response. The forms include:

- **Proposal Response Forms**. The Vendor is required to use the Proposal Response Forms contained in this volume for their proposal response. This volume contains response information from the Vendor related to qualifications and references, functional requirements, hardware and network requirements, contractual requirements and price proposal. All proposal responses must be entered into the electronic form (MS Word) provided as part of the Vendor's proposal response. Electronic images or .pdf versions of these files will not be accepted as compliant.

- Vendors may bid with either or both of the following system integration options:
  - o **On-Premise** – The Consortium purchases software and implementation services from the Vendor, but elects to implement on the Consortium's infrastructure.
  - o **Vendor-Hosted SaaS** – The Consortium purchases the Vendor's SaaS services. Sections corresponding to each proposal type are labelled in accordance to this (On-Premise solutions must respond to all sections with numbering that includes A, while Vendor-Hosted SaaS solutions should respond to all sections with numbering including B). Vendors capable of providing either solution should respond accordingly to both.

- **Functional Requirements Response Forms.** The Vendor is required to use the Functional Requirements Response Forms contained in this volume for their proposal response. This volume contains detailed descriptions of all technical and functional specifications and requirements for the proposed system. These forms can be found in Attachment A2 – Functional Requirements Response Forms and include:

  - FRR – General System
  - FRR – Computer Aided Dispatch System
  - FRR – Records Management System
  - FRR – Detention Management System

  All Technical proposal responses must be entered into the electronic form (MS Excel) provided as part of the Vendors proposal response. Electronic images or .pdf versions of these files will not be accepted as compliant.

- **Consortium Required Forms –** The Vendor is required to complete any attached Consortium Required Forms located in Attachment A3.

Item	Instructions
Cover Letter	Submit a copy of the cover letter on your letterhead signed by the responsible official in your organization, certifying the accuracy of all information in your proposal, and certifying that your proposal will remain valid for a period of two hundred seventy (270) calendar days from the date of proposal opening. It should also include the names of individuals within the company to contact for technical, pricing, and contractual questions.
Use the Proposal Response Forms to respond to the following sections:	
Section 1.0: Qualifications and References Response	Use the attached MS Word file titled, **"Proposal Response Forms,"** to respond to this section.
Section 2.0: Functional Requirements Response	The requirements for all of the software systems covered by this procurement are described in the MS Word file titled **"Proposal Response Forms".** Respond directly into MS Word

Item	Instructions
	File. Respond to the functional requirements by entering directly into the MS Excel spreadsheets under **Functional Requirements Response Forms”**.
Section 3.0: Infrastructure Requirements Response	Respond to RFP Section 3. Use the attached MS Word file titled **“Proposal Response Forms”** to respond to this section. Where the RFP asks for lists or detailed supplemental information, place that information in the Vendor Supplemental Information at the end of the section. Include a schematic of the system.
Section 4.0: Service and Maintenance Requirements Response	Respond to RFP Section 4. Use the attached MS Word file titled **“Proposal Response Forms”** to respond to this section. Where the RFP asks for lists or detailed supplemental information, place that information in the Vendor Supplemental Information at the end of the section.
Section 5.0: Performance Requirements Response	Respond to RFP Section 5. Use the attached MS Word file titled **“Proposal Response Forms”** to respond to this section. Where the RFP asks for lists or detailed supplemental information, place that information in the Vendor Supplemental Information at the end of the section.
Section 6.0: Implementation Requirements Response	Respond to RFP Section 6. Use the attached MS Word file titled **“Proposal Response Forms”** to respond to this section. Place the following information in the Vendor Supplemental Information: ▪ Proposed Implementation Schedule; ▪ Implementation Project Plan; and ▪ Resumes for the persons who will work on this project.
Section 7.0: Contractual Requirements & Agency Forms	Review Attachment A4 – Consortium Terms and Conditions in this section. Note any exceptions in Section 7 of the **“Proposal Response Forms”.** Include completed Certifications & Assurances Form in your proposal, labeled as Attachment A3.
Section 8: Price Proposal	Follow the instructions in RFP Section 8 for preparing cost summary, explanatory notes, and back-up details. Use the attached MS Word file titled **“Proposal Response Forms”** to respond to this section.
Attachments:	Appendix 1 - Brochures / specification / contracts for proposed products as necessary (if any)

1.8 Evaluation & Award Process

The Consortium will conform to the evaluation and award process below, subject to change at the consortium's discretion.

- Proposals will be objectively evaluated by a committee based on conformity to the specifications as determined by the evaluation criteria in RFP Section 1.9, and a short list will be developed;
- Short-listed Vendors may then be evaluated based on references, oral presentations, demonstrations and site visits to similar installations. Written responses to queries for further clarification may also be required;
- Final scoring will be based on the criteria given in Paragraph 1.10;
- Best and Final offers may be requested from the Short-listed Vendors; and
- Contract negotiations will begin immediately with the selected Vendor.

1.9 Initial Evaluation Criteria

The Consortium will evaluate Vendors' proposals based on the completeness and quality of their responses to all sections.

Section	Description	Value
1.0	Qualifications & Experience	10
2.0	Functional Requirements Proposal	30
3.0	Infrastructure Proposal	10
4.0	Service & Maintenance Proposal	10
5.0	Performance Proposal	5
6.0	Implementation Proposal	15
7.0	Contractual Proposal	5
8.0	Price Proposal	15

1.10 Final Evaluation

Once a short list of Vendors has been invited to continue with the process, other Vendors will be notified. The short list of Vendors will be engaged to demonstrate their products; based on their performance in the demonstration, references and site evaluations, up to two Vendors will be asked to participate in a best and final process.

Element	Value
Initial Evaluation Criteria (Table Above)	100
Demonstration	30
References / Site Evaluation	20
Total	**150**

2.0 BACKGROUND AND FUNCTIONAL REQUIREMENTS

2.1 Introduction

This section provides consortium operational background and detailed description of the systems being replaced by those systems outlined in Section 1.1 above.

2.2 Current Environment

2.2.1 Application Systems Overview

The Consortium's current public safety systems architecture consists of computer-aided dispatch, law enforcement records management, mobile data computing systems, and detention management acquired from CRIMES over a decade ago. The system operates in a traditional MS Windows-based client/server environment. The system is disjointed with minimal interfaces, which makes field operations very difficult and has extensive limitations relative to field reporting and analytics. In addition, each City hosts their own version of CRIMES, which are all on different versions, making it very difficult to share important data between agencies. This lack of functionality results in a system that can only perform the basic, everyday tasks of the departments, without the interoperability the Consortium is looking to achieve. In addition, there is currently no regional GIS map that the patrol officers can utilize for joint operational efforts. This integrated map is a major goal for this project. The applications interaction diagram is shown below to reflect the current environment.

Multi-City Public Safety Consortium
Current Applications Environment
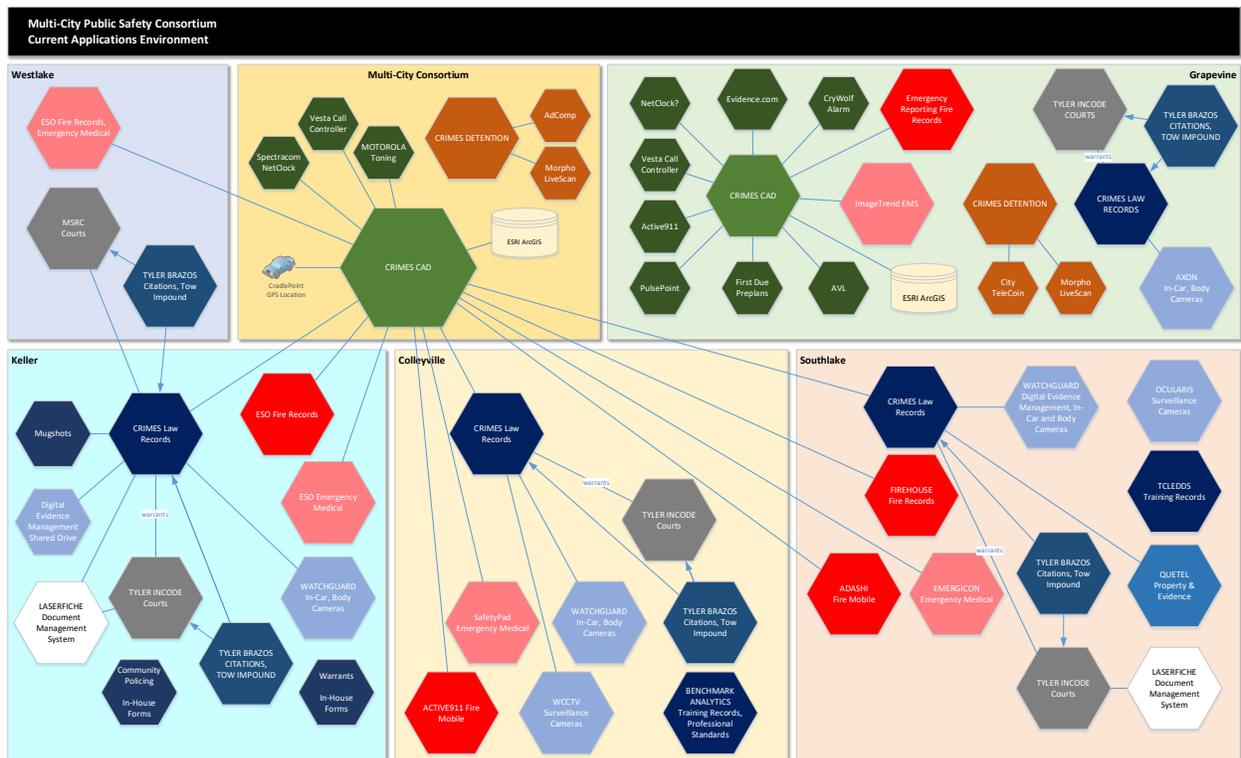
Although the CRIMES CAD/RMS has a few developed customized features, it underperforms in many areas that the departments need due to several reasons: lack of support from the Vendor, lack of upgrades, and lack of key functionality that is standard in today's modern systems. This has prompted the department to begin looking at new options which will enable them to integrate workflows, have robust field reporting capabilities, and provide real-time analytics.

Several 3rd party applications are utilized in addition to the primary CRIMES system. Some of these applications are critical to the overall service delivery of the organization and some should be replaced with the functionality of the new system. Analysis of the new system's functionality will be necessary to see what applications can be either integrated or replaced by the new CAD/RMS. These applications are summarized below.

2.2.2   Interfaces and Migration Plan

The Consortium uses the following ancillary systems to interface with the current CRIMES system. The chart below describes the interface as well as shows the preliminary migration plan to the new public safety system. These interfaces are also summarized in the FRR – General System spreadsheet for the proposer to answer whether they can or cannot interface with the application and input the cost of each application to develop the interface with the proposed CAD/RMS.

*Legend for Current Applications	
Legend Code	Description
Replace	The City's intent is to replace this application with the selected solution
Consider	The City is considering the replacement of this application with the selected solution, based on the strength of the finalist Vendor offering and cost/benefit of the replacement module.
Maintain	The City is intending on retaining the application, not replacing it thru this effort.
Interface	The City is intending on keeping the application and interfacing/integrating it with the selected solution.

Current CAD/RMS/JMS Application/ Interface	Application & Version	Notes/Comments	Replace or Interface
The City of Keller			
CAD			
▪ Radio System	Motorola / Fort Worth Radio System	Northeast Tarrant County Consortium	Interface
▪ Call Taking/Dispatching	CRIMES 6.8 CAD		Replace
▪ Message Switch	N/A		N/A
▪ Timeclock	Spectracom Netclock #9383	double check on model	Interface
▪ Alerting	N/A		N/A
▪ Mapping	CRIMES AVL link with GIS	Cradle Point Routers in vehicle	Interface
▪ Call Controller	Vesta 7.2 SP1 HF1	911, 10-digit, Admin call taking lines	Interface
▪ Toning	Motorola / Fort Worth Radio System	Northeast Tarrant County Consortium	Interface
▪ Reporting	CRIMES 6.8		Replace

Current CAD/RMS/JMS Application/ Interface	Application & Version	Notes/Comments	Replace or Interface
Police Records			
▪ Report Entry/Approval	CRIMES 6.8		Replace
▪ Case Management	CRIMES 6.8		Replace
▪ Property & Evidence	CRIMES 6.8		Replace
▪ Digital Evidence Management	In-House Shared Drive or CD/DVD		Replace
▪ Crime Analysis	CRIMES / CRIS Accident Reporting		Replace
▪ Mugshots	Shared Drive		Replace
▪ Warrants	In-House Forms		Interface
▪ Community Policing	N/A		Replace
▪ Tow-Impound	Brazos/Tyler Technologies		Interface
▪ UCR/NIBRS	CRIMES 6.8		Replace
▪ Training Records	In-House Forms		Replace
▪ Professional Standards	In-House Forms		Replace
Police Mobile			
▪ CAD Mobile	CRIMES 6.8		Replace
▪ Field-based Reporting	CRIMES 6.8		Replace
▪ E-Citation	Brazos/Tyler Technologies		Interface
Fire			
▪ CAD Fire Mobile	CRIMES 6.8		Replace
▪ Fire Records	ESO Solutions	Go Live Jan. 2020	Interface
▪ Fire Mobile	CRIMES 6.8, Active 911, Pulse Point		Replace
▪ EMS	ESO Solutions		Interface
Detention			
▪ Booking	CRIMES 6.8		Replace
▪ Identification	Livescan		Interface
▪ AFIS Interface	Safran MorphoTrust		Interface
▪ Inmate Tracking	CRIMES 6.8		Replace
▪ Inmate Property	CRIMES 6.8		Replace
▪ Medical	CRIMES 6.8		Replace
▪ Reporting	CRIMES 6.8		Replace
Other Systems			
▪ In-Car Camera	WatchGuard		Interface
▪ Body Camera	WatchGuard		Interface
▪ Surveillance Cameras	Ocularis		Interface
The City of Colleyville			
Police Records			
▪ Report Entry/Approval	CRIMES		Replace
▪ Case Management	CRIMES		Replace
▪ Property & Evidence	CRIMES		Replace
▪ Digital Evidence Management	CRIMES		Replace
▪ Crime Analysis	CRIMES		Replace
▪ Mugshots	CRIMES		Replace
▪ Warrants	Incode V10		Replace
▪ Community Policing	N/A		Replace
▪ Tow-Impound	Brazos		Interface
▪ UCR/NIBRS	CRIMES		Replace

Current CAD/RMS/JMS Application/ Interface	Application & Version	Notes/Comments	Replace or Interface
▪ Training Records	Benchmark Analytics		Interface
▪ Professional Standards	Benchmark Analytics		Interface
Police Mobile			
▪ CAD Mobile	CRIMES		Replace
▪ Field-based Reporting	CRIMES		Replace
▪ E-Citation	Brazos		Interface
Fire			
▪ CAD Fire Mobile	CRIMES web version		Replace
▪ Fire Records	Emergency Reporting		Interface
▪ Fire Mobile	CRIMES 6.7, First Due, Active 911, Pulse Point		Replace
▪ EMS	SafetyPAD		Interface
Other Systems			
▪ In-Car Camera	WatchGuard		Interface
▪ Body Camera	WatchGuard		Interface
▪ Surveillance Cameras	WCCTV		Interface
The City of Southlake			
Police Records			
▪ Report Entry/Approval	CRIMES 6.8		Replace
▪ Case Management	CRIMES 6.8		Replace
▪ Property & Evidence	QueTel		Consider
▪ Digital Evidence Management	WatchGuard Evidence Library	EL4 version 4.4.3	Interface
▪ Crime Analysis	CRIMES 6.8		Replace
▪ Mugshots	CRIMES 6.8 (Jailman)		Replace
▪ Warrants	Incode & Laserfiche		Interface
▪ Community Policing	N/A		Replace
▪ Tow-Impound	N/A		N/A
▪ UCR/NIBRS	CRIMES 6.8		Replace
▪ Training Records	TCLEDDS		Interface
▪ Professional Standards	IAPro 7.1/BlueTeam		Replace
Police Mobile			
▪ CAD Mobile	CRIMES 6.8		Replace
▪ Field-based Reporting	CRIMES 6.8		Replace
▪ E-Citation	Brazos v1.91-261-g97d715ee		Interface
Fire			
▪ CAD Fire Mobile	CRIMES 6.8		Replace
▪ Fire Records	FireHouse RMS		Interface
▪ Fire Mobile	Adashi		Replace
▪ EMS	Emergicon		Interface
Other Systems			
▪ In-Car Camera	WatchGuard 4.4.3		Interface
▪ Body Camera	WatchGuard 4.4.3		Interface
▪ Surveillance Cameras	Ocularis 7.8		Interface
The City of Westlake			
Fire			
▪ CAD Fire Mobile	CRIMES		Replace
▪ Fire Records	ESO		Interface
▪ Fire Mobile	CRIMES		Replace
▪ EMS	ESO		Interface

Current CAD/RMS/JMS Application/ Interface	Application & Version	Notes/Comments	Replace or Interface
The City of Grapevine			
CAD			
▪ Radio System	Motorola 7.18		Interface
▪ Call Taking/Dispatching	CRIMES 6.5.4		Replace
▪ Message Switch	CRIMES 6.5.4		Replace
▪ Timeclock	Spectracom Netclock 9383		Interface
▪ Alerting	CRIMES 6.5.4 & Rave		Replace
▪ Mapping	IT Nexus/Crimes		Replace
▪ Call Controller	Airbus Vesta		Interface
▪ Toning	Motorola MCC 7500 v7.18		Interface
▪ Reporting	CRIMES/SQL SSRS/Crystal	Keep SQL/Crystal caps	Consider
▪ Alarm Management	Cry Wolf		Interface
Police Records			
▪ Report Entry/Approval	CRIMES 6.7		Replace
▪ Case Management	CRIMES 6.7		Replace
▪ Property & Evidence	CRIMES 6.5.7		Replace
▪ Digital Evidence Management	Axon Evidence.com		Interface
▪ Crime Analysis	CRIMES 6.7		Replace
▪ Mugshots	CRIMES 6.7		Replace
▪ Warrants	Incode		Interface
▪ Community Policing	N/A		Replace
▪ Tow-Impound	Brazos		Interface
▪ UCR/NIBRS	CRIMES 6.7		Replace
▪ Training Records	MdE Adore		Consider
▪ Professional Conduct	IA Pro/Blue Team		Interface
Police Mobile			
▪ CAD Mobile	CRIMES 6.7		Replace
▪ Field-based Reporting	CRIMES 6.7		Replace
▪ E-Citation	Brazos		Interface
Fire			
▪ CAD Fire Mobile	CRIMES 6.7		Replace
▪ Fire Records	Emergency Reporting	Web based	Interface
▪ Fire Mobile	CRIMES 6.7, First Due, Active 911, Pulse Point	Web based	Consider
▪ EMS	Image Trend	Web based	Interface
Detention			
▪ Booking	Crimes 6.7.2		Replace
▪ Identification	Livescan TPE-5938-ED	Set to be replaced	Interface
▪ AFIS Interface			Interface
▪ Inmate Tracking	Crimes 6.7.2		Replace
▪ Inmate Property	Crimes 6.7.2		Replace
▪ Medical	Crimes 6.7.2		Replace
▪ Reporting	CRIMES/SQL SSRS/Crystal		Replace
Other Systems			
▪ In-Car Camera	Axon, Fleet 2		Interface
▪ Body Camera	Axon, Body 3		Interface
▪ Surveillance Cameras	Pelco Video Expert		Interface

Most of these applications, although critical to the overall functionality of the organization, are not integrated into a logical workflow. The consortium's application architecture is characterized with varied systems for most of the Dispatch and Records functions with limited integration amongst them. Most of the current processes are not integrated with CRIMES which must be manually inputted each day.

Further analysis of the organization's functional processes shows that the lack of integration forces the patrol units, CID, and Street Crimes to operate in a reduced state of efficiency primarily due to the extensive paper tracking, manual workflows, and re-entry of information into multiple systems. A new integrated system with fewer interfaces will fix these problems and create more efficient workflows.

The lack of effective reporting or analytical functionality extremely limits the Department's vision to be transparent and informative to its citizens or officers. This means that with the current system, the Department is not able to show crime statistics, hot spots or trend analytics to their patrol officers, further putting them at risk. With a new CAD/RMS/Mobile system, officers will have the information they need in a timely manner in order to give the best possible service to the Cities' citizens.

2.2.3 Current Infrastructure and Technical Environment

As part of the Consortium's assessment, the following technical areas were examined to identify any challenges that could inhibit the new system's effective installation, deployment and use. The proposed system needs to comply with these standards and integrate with the hardware already used by the Consortium.

Question	Response				
Operating Systems (OS) & Related Software					
	Keller	Colleyville	Southlake	Westlake	Grapevine
▪ Desktop operating system(s)	Windows 10	Windows 10	Windows 10	Windows 10	Windows 10
▪ Mobile device operating system(s)	iOS/Android/ Windows 10	iOS/Android	iOS		iOS/Android/ Windows 10
Hosting City					
▪ Server operating system(s) and version levels	Keller: Windows Server 2016 and 2019 Grapevine: MS Server 2012, 2016				
▪ Relational database	Keller: SQL Server 2016 Grapevine: MS SQL				
▪ Geographic information system (GIS)	Keller: ESRI Grapevine: ESRI				
▪ Business application environment	Keller: Microsoft Grapevine: Microsoft				
▪ Document management system	Keller: Laserfiche 10.2 Grapevine: Laserfiche 10.4				
Hardware					
	Keller	Colleyville	Southlake	Westlake	Grapevine
▪ Server hardware (VM, hypervisor), version level	VMware vSphere 6.5	VMware 6	VMware vSphere 6.7	N/A	Vcenter
▪ Desktop hardware	55	Dell/ Windows 10	70	4	151

| Question	Response				
▪ Mobile devices (MDTs, tablets, ticket writers)	28 MDTs 14 tablets 18 TW	10 iPads 14 MDTs 14 TW	52 iPads 54 TW	8	20 Surface 60 Getac 25 iPads
Data Center					
Hosting City					
▪ Physical space, rack space, and environmentals (i.e., AC, power) in the data centers to accommodate the new system running concurrently with the old system during install and testing	Keller: Yes, sufficient space Grapevine: Yes, sufficient space				
▪ Backups and automation process	Keller: Data stored on SAN is replicated to DR site hourly. All data is backed up nightly and replicated to DR site. Grapevine: Data is backed up off-site using One Safe Place nightly. A copy is stored on-site and off-site. Veeam is used to get full virtual server backups to a secondary storage unit nightly.				
▪ Disaster recovery measures	Keller: DR site at City facility. Grapevine: Some functions are stored in the cloud. DR is on an application basis. Azure AD setup and in use.				
Network					
Hosting City					
▪ Network equipment (i.e., switches, routers)	Keller: Core Router: Cisco Nexus 9504, PD router: Cisco 4507, Secondary switches: Cisco 3650 Primary Firewall: Cisco ASA5525, IPS/IDS: Palo Alto 3220 Grapevine: Cisco Nexus 7706, 9396PX, 9396TX, Catalyst 4510 2960X, Cisco Rtr 4331, Sophos 330 UTM				
▪ Internet Point of Presence (POP)	Keller: City has 2 internet service providers located at primary Town Hall data center. Primary is 200x200, secondary is 150x150. Load balanced with a Peplink Balance 580. Grapevine: 2, but the locations are in the same buildings.				
	Keller	Colleyville	Southlake	Westlake	Grapevine
▪ Participating agencies secondary Internet POP	Yes	Yes	Yes	Yes	Yes
Other					
Hosting City					
▪ Field Automation Capabilities	The Consortium has minimal field automation today. The Consortium is open to deploying field automation devices where an obvious improvement in efficiency and effectiveness will result.				
▪ Customizations	The Consortium wants to purchase a system that is self-configurable, commercial off-the-shelf (COTS) system. It is not interested in customizations or systems that require teams of software engineers to configure the system.				

The current storage platforms are sufficient to support a new system. In order to make the system fully disaster resilient, the RMS will need to be stored on a separate server at a County location. If the new CAD/RMS system is to be stored locally, the secondary data center will also have to be utilized in order to satisfy these prevention measures.

2.2.4 Current Network Environment

There are multiple key components of the current infrastructure. These are 9-1-1 Service; Computer Aided Dispatch (CRIMES); Law Enforcement Records Management (CRIMES); the Data Network; and, the Radio Network. These systems are mainly housed in the PD building and the Town Hall at the cities of Keller and Grapevine with some other peripheral systems located in other buildings throughout the consortium. This is to provide sufficient disaster recoverability and overall security to the information.

Keller (Main Hosting Site) Network Infrastructure

The current network within the City of Keller (main hosting site for the Consortium) is solid and provides dependable service. The Town Hall data center and the DR site are linked with fiber, which should be sufficient to run the system in the event of an emergency. The Town Hall has two internet Point of Presences (POPs), both in the same building. This could be a risk, if a disaster destroyed the building, therefore leaving the City without internet. Load balancing is performed through a Peplink Balance 580. The current environment for Keller, the main hosting site for the system, is illustrated below. The CAD system communicates directly to the mobile devices in the cars over public carrier wireless.
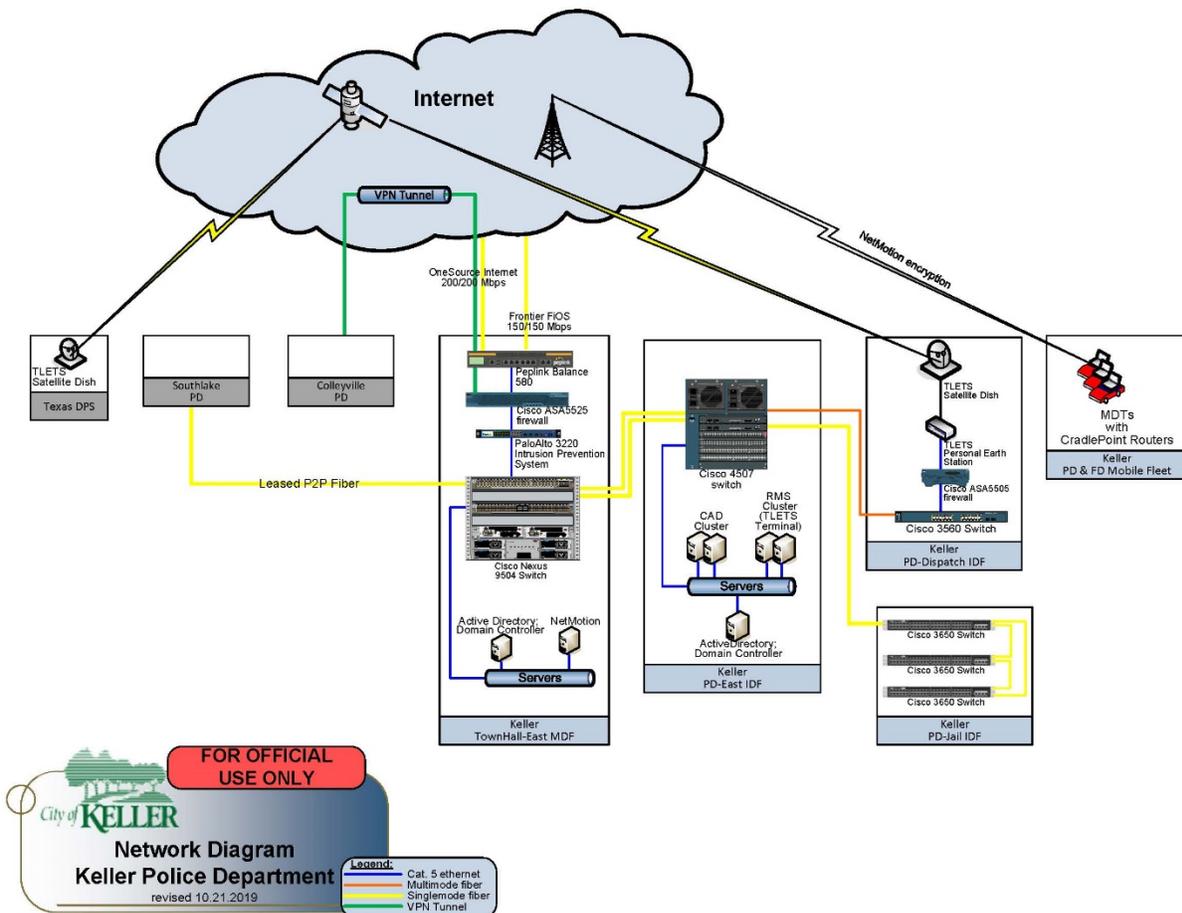
Overall, the City of Keller has built an extensive network infrastructure that can handle a locally hosted or cloud solution modern CAD/RMS system. The only recommendation for the network to become more disaster resilient and be prepared for implementation of the new system is to have the backup data center (for the CAD/RMS) located in a neighboring city at least 5 miles apart from the Keller main data center. This is where backups of all files should be stored.

Grapevine Network Infrastructure

Shown below is the network diagram for the City of Grapevine. (outside the Consortium but will still share GIS data for the regional map). The City of Grapevine's network infrastructure is also very solid and should be able to handle either a locally hosted or cloud solution modern CAD/RMS system. The only point of concern is that the first and second internet PoPs are located in the same building. Ideally, these two PoPs should be separated into two different sites so that if one fails due to a building issue, the other can come online and continue internet service for the Department.
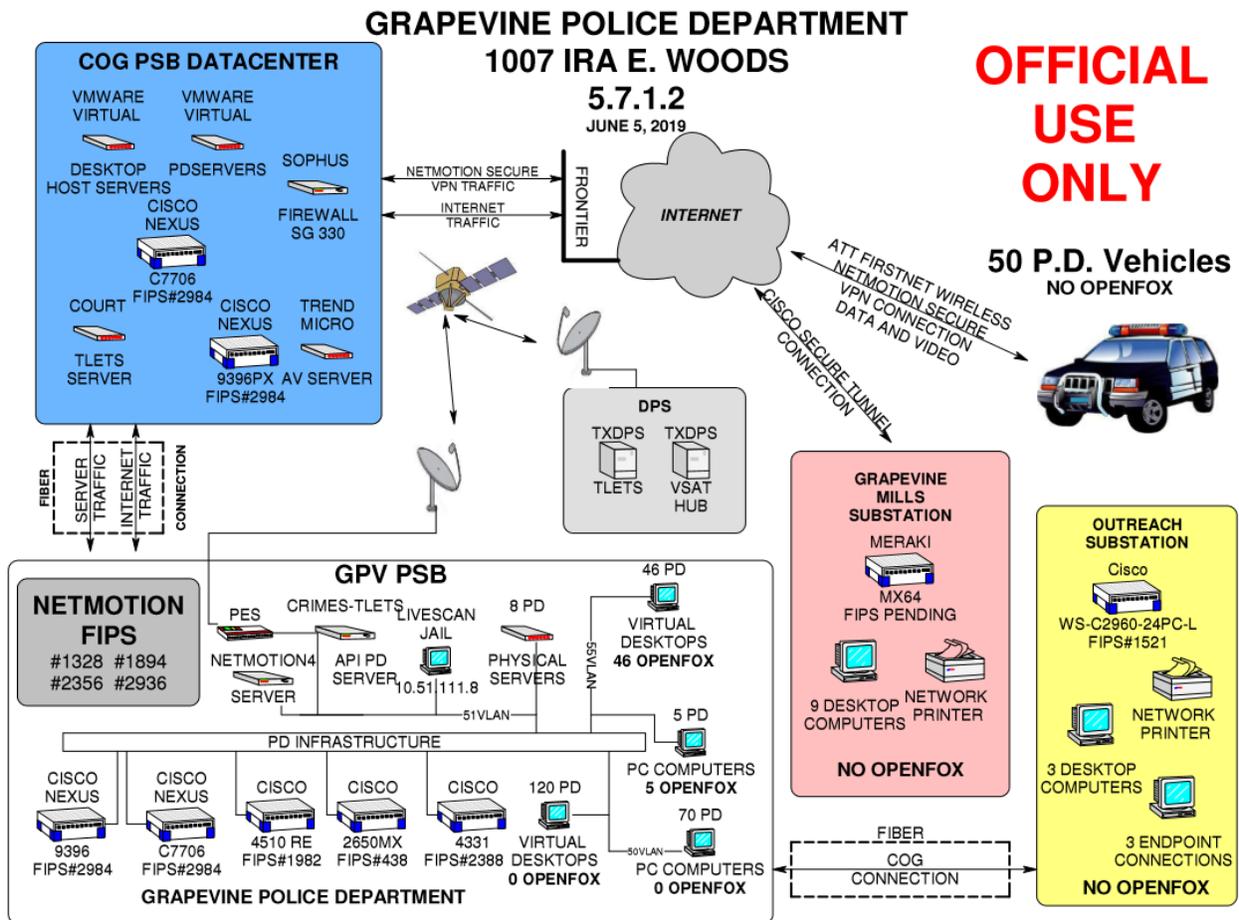
2.3   Migration from the Current System

The Consortium currently uses the CRIMES CAD/RMS system. The new system must be able to utilize accumulated data from the systems currently in place. The migration path from the existing systems must include any necessary modifications to currently existing systems which are not being supplanted by the new system as well as any necessary data conversion and importation from current systems.

Proposals should include an explanation on data conversion. Specifics about present systems can be provided upon request. Sizing parameters are provided below.

Table 2.2 Sizing Parameters

| Sizing Statistics		Current				
City Statistics						
		Keller	Colleyville	Southlake	Westlake	Grapevine
City Total Population		48,000	25,487	29,440	1,500	54,000
Jurisdictional Area (Square Miles)		18.42	13.1	22.5	6.68	32 (4 water)
Total 911 Calls per Year		15,000	7,000	17,183	2,250	33,000
Number of Users per System						
		Keller	Colleyville	Southlake	Westlake	Grapevine
# of Call Takers/ Dispatchers	Total Licenses	20	Keller	Keller	Keller	20
	Simultaneous	7	Keller	Keller	Keller	6
# of CAD Mobile Users	Total Licenses	58	46	75	8	105
	Simultaneous	25	20	52	4	25
# of Law FBR Mobile Users	Total Licenses	58	46	75	0	105
	Simultaneous	25	20	52	0	25
# of Law RMS System Users	Total Licenses	51	51	75	0	150
	Simultaneous	25	27	52	0	30
# of DMS System Users	Total Licenses	12	Keller	Keller	Keller	20
	Simultaneous	5	Keller	Keller	Keller	6
Police Departments						
		Keller	Colleyville	Southlake	Westlake	Grapevine
Full time sworn/uniformed		51	44	74	N/A	101
Full time civilians		35	7	7	N/A	44
Number of Police Districts		5	4	4	2	9
Number of Police Stations		1	1	3	0	2
Number of Police Vehicles with MDTs		15	15	24	0	40
Number of Dispatched Calls per Year		15,000	7,000	12,808	1,700	26,000
Number of Incident Reports/Cases per Year		1,110	1,700	2,619	135	5,500
Number of Arrests/Bookings per Year		700	700	2,473	200	1,300
Number of Traffic Citations per Year		12,000	5,4000	13,806	8,600	12,800
Fire Departments						
		Keller	Colleyville	Southlake	Westlake	Grapevine
Full time sworn/uniformed		56	44	69	17	108
Full time civilians		1	1	4	1	4
Number of Fire Stations		3	3	3	1	5
Number of Fire Vehicles with MDCs		14	7	17	7	18
Fire – # of Dispatched Calls per Year		3,900	1,800	3,376	550	6,192

2.4 Future Direction

2.4.1 Application Systems

The Consortium has chosen to invest in a next generation integrated Public Safety application suite in order to streamline the information flow within the Consortium and improve the efficiency of its workforce. In addition, the Consortium aims to incorporate state-of-the-art self-service capabilities for its citizens.

The Consortium is embracing digital government with a focus on improved field-based reporting and efficient operations. In the time since acquisition of the organization's CAD/RMS, processes and internal demands have evolved and expanded, creating functional gaps between the system's available capabilities and those being demanded by users. The Consortium is also addressing the changing expectations of its citizens for effective interaction.

In addition, the Consortium believes that planned, prudent investment in technology that enables the citizenry to conduct transactions with minimal staff intervention will also help to better utilize existing staffing levels to meet the demands from their citizens.
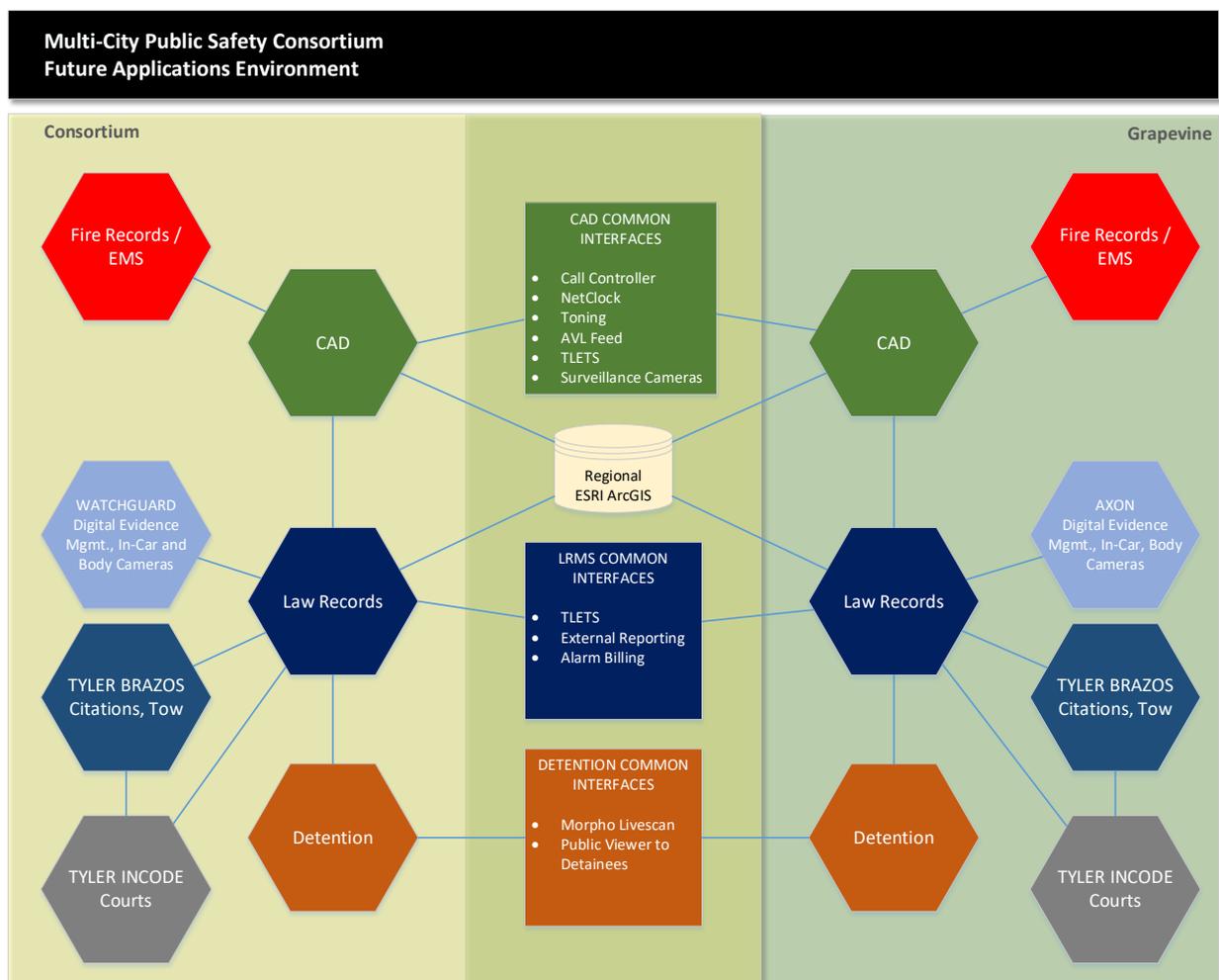
A modern CAD/RMS can integrate with related computerized systems to retrieve relevant data and incorporate that data into the CAD/RMS. This integration provides the obvious benefit of reducing data input time for the users. Moreover, by bringing the data directly from the source data systems, data input errors can be minimized, thus maximizing the value received from these systems as well.

The coordinated access to information along with digital document workflow capabilities expedites the case flow by digitally replacing the existing paper routing processes and providing easy archiving and retrieval of key documents. This not only shortens the case process time but also reduces the need for paper files.

2.4.2   Infrastructure and Network

It is expected that if a self-hosted option is chosen, the primary applications will be installed in the Cities of Keller's and Grapevine's main data centers. Any ancillary or additional systems that may be required (i.e., imaging server) will also be installed at these data centers, which also houses most of the users of the integrated system. Alternatively, a Cloud-based option will be operated from the Vendor's data center.

Nearly all users of this system on the Local Area Network are supported by fiber. It is expected that the Vendor will review the Consortium's network and identify any network concerns it might have that would impede it from meeting the performance requirements specified in Section 5.

The mission critical applications are vital to the ongoing operation of the organization, and a disaster recovery site is available today, offsite. The Cities of Keller and Grapevine both currently utilize a backup site to store its mission critical applications. It is requested the vendor propose a DR plan (both cloud and on-site) solution. Please use the **A1 - Proposal Response Forms**, Section 3.3A.3, OP: Disaster Recovery Solution or Section 3.3B.3, SaaS: Disaster Recovery Management to propose this Plan and give any details regarding Consortium requirements for the Plan.

If the solution provided is not Cloud-based, rack space for equipment specified by the Vendor will be provided. The Vendor will provide specifications for its equipment as well as the servers used to support the system. These systems will be installed by the Cities of Keller and Grapevine at their respective data centers.

2.4.3   System Backup

The proposed solution (both cloud and on-site) must provide for the ability to perform a full backup of the system to a local storage system housed at the Keller/Grapevine data centers. All systems must remain fully operational while the backup is occurring, without any effect to the live operation.

Please describe the proposed architecture to accomplish this, which could include: a backup to the City of Keller/Grapevine storage systems and/or specifications for a SAN and SAN backup design that is integrated with the application systems. Proposed equipment must enable a full or partial restoration of all data files. Vendor must describe method of storage backup and restoration proposed. Pricing should include all necessary

licensing costs/fees for all applicable backup software. Proposals leveraging the existing infrastructure, including certification that the above requirements are met, will be favored.

2.5   Functional Requirements

The Consortium will replace the existing CRIMES CAD/RMS system to include all Call Taker, Dispatch, CAD Administration, Reports Management, Crime Analysis, Case Management, Civil Process, Mobile Field Based Reporting, and Detention Management functionality. Core components of the optimal design for the Consortium include the Overall Functional Requirements identified in Section 2.5.1, below, as well as the Software Functional Requirements referred to in Section 2.5.2, below, and identified specifically in the Functional Requirements spreadsheets.

2.5.1   Overall Functional Requirements

In evaluating overall functional requirements, the Consortium will consider the following:

- **Industry Standard Architecture** – The architecture will be flexible and will be based on widely accepted standards. This will make it easier to integrate/interface the mission critical applications and other internal/external modules. It can also improve the systems' ability to interoperate with a number of modern technologies, such as:
  - o Document and imaging management systems
  - o Powerful and flexible ad hoc reporting tools
  - o Field automation and mobility tools
  - o Web-based self-service functions for employees and citizens
  - o Geographic information systems (GIS).

- **High Availability** – The architecture, will need full redundancy and fail-over capabilities, and should contain no single point of failure.

- **Secure** – The system will incorporate the elements of authentication, authorization, encryption, monitoring/detection, and physical security that adhere to industry standards.

- **Web-Based Architecture** – The systems will take advantage of the integrating capabilities of the web services architecture. This will provide many users the ability to Intergraph with the applications via a Web browser.

- **Scalable** – Scalability will be critical to support expansion and workload variability.

- **Full Integration** – The system must act as a single CAD/Records Management System with required data flowing between modules or systems as required to act as a single system. Data that is entered once must update all applications and relevant portions of associated systems.

- **Workflow Functionality** – Fully-integrated field applications (i.e., CAD Mobile, Field Based Reporting) flowing data to all relevant portions of associated systems. Electronic workflow enables the specification of business rules, roles, and routings that can be used to automatically route electronic documents, such as budgets or

purchase acquisition requests, to supervisors and management for notification, review, and approval.

- **Relational Database Management System** – The Consortium has standardized on SQL Server for relational database technology since it supports ready interface and integration among systems. The new system will utilize this technology and make the database accessible to the Consortium.

- **Data Integrity and Validation Tools -** The system will facilitate the validation of the key parameters of address and personal identity. The system will validate address entries through integration with the system geo-database.

- **External Integration Flexibility** – The system will adhere to the use of industry standards. This will make it easier to integrate the mission critical systems and to share data with external systems.

2.5.2   Software Functional Requirements

The requirements for the software systems covered by this procurement are described in the attached (4) MS Excel spreadsheets:

- **A2 - Functional Requirements Response Forms**

    o   FRR – General System
    o   FRR – Computer Aided Dispatch System
    o   FRR – Records Management System
    o   FRR – Detention Management System

For each specification, Vendors will be required to provide one of four standard responses. Respond directly into each spreadsheet; failure to do so may cause your response to be considered non-compliant.

For the purposes of response, use the following definitions of your four standard response options:

- **Compliant** - Proposed system meets or exceeds the requirement. This is the only response category that will result in full credit for complying with this requirement.
- **Alternative Method** – The requirement is met by the proposed system but uses a method (i.e., entry screen, workflow, form[s]) that differs from that specified in the requirement. Detail the method to be used to meet the requirement.
- **Modification Required** – A modification must be provided to comply with this requirement. The requirement will be provided with the initial install of the software. Specify the modification to be made and include cost, if any, in the pricing proposal.
- **Non-Compliant** - The proposed system does not meet the requirements and will not do so within twelve months of the RFP release date.

Explanations of responses should be entered into the "Comments" field if you can reasonably do so; if not, include the explanation in the "**Proposal Response Forms**," Section 2. Submit any additional information in the attached "**Proposal Response Forms**." Include all these documents as part of your proposal submission.

3.0   INFRASTRUCTURE REQUIREMENTS

3.1   Introduction

This section describes the servers, peripherals, data communications equipment, hosting environments, performance and reliability requirements, and workstations required for operation of the proposed system(s) to support the application software requirements, volumes, and processing characteristics defined previously.

Use Section 3 to develop an understanding of the existing and future environment. Respond to each of the points as described in the section by using the attached response forms. Vendor-Hosted and On-Premise solutions should respond to their respective sections as labelled, and Vendors able to provide either option should respond to both sections. For each of the sections and subsections state in the **Proposal Response Forms** whether you meet the requirements with explanation of your compliance or non-compliance.

3.2   System Architecture

Provide an introductory narrative of how the proposed system meets the overall objectives and functional requirements. It should cover the main features and benefits that distinguish your system.

Vendors may bid with either or both of the following system integration options:

A. **On-Premise** - The Consortium purchases software and implementation services from the Vendor, but elects to implement on the City's infrastructure; or
B. **Vendor-Hosted SaaS** – The Consortium purchases the Vendor's SaaS services.

Sections corresponding to each proposal type are labelled in accordance to this (On-Premise solutions must respond to all sections with numbering that includes **A**, while Vendor-Hosted SaaS solutions should respond to all sections with numbering including **B**). Vendors capable of providing either solution should respond to both.

For both On-Premise and Vendor-Hosted solutions, subsequent to the introductory paragraph, expand upon your plan for future system enhancements; your investment plans are considered to be a reflection of your company's commitment to the long-term viability of the system architecture. The installed system must be capable of expansion in a modular and incremental fashion.

3.2A   On-Premise

If proposing an On-Premise solution, your response should include a **System Diagram** that depicts the overall design of the system.

3.2B   Vendor-Hosted SaaS

If proposing a Vendor-Hosted solution, your response should include a **Multi-Data Center Topology Diagram** depicting the Vendor's primary and backup data center locations and

the method by which the connection is routed to primary data center as well as to how the connection is rerouted to the City in the event of a Catastrophic Service Interruption.

3.3 Infrastructure Specifications or Hosting Environment

The intent is to pursue one of two paths and desires proposals for both if available:

A. Purchase software and services from the vendor to install on the City's servers (On-Premise), elaborated in Section 3.3A below.

B. Purchase the vendor's Software-as-a-Service (SaaS), elaborated in 3.3B below.

Vendors should utilize the response forms sections for either 3.3A for On-Premise proposals, 3.3B for Vendor-Hosted SaaS proposals, or both if each option is available.

3.3A Infrastructure Specifications [For On-Premise Proposals]

3.3A.1 Server Specifications

The Vendor is to specify the required servers that support the application performance. The Vendor should specify the application servers that they recommend that could be used in a virtual environment.

3.3A.2 Operating System and Related Software

The Consortium has standardized on Microsoft Windows. The future solution must be capable of supporting real-time applications that are actively supported by the CPU hardware manufacturer. Licenses for the operating systems will be received. All proposals must provide the name and version number of the proposed operating system. Proposals that incorporate a non-Microsoft operating system solution must contain an explanation for the choice of operating systems and must indicate whether it is the Vendors intention to migrate to a Windows environment in the future.

3.3A.3 Disaster Recovery Solution

3.3A.3.1 Identify your business continuity and disaster recovery options, with their respective costs.

3.3A.3.2 Identify how and where the disaster recovery data may be stored.

3.3A.3.3 Describe the replication and synchronization strategy for restoring the complete system (both data and application software) within the Vendors operating environment (i.e., intra and inter data center replication).

3.3A.3.4 Will the Vendor offer a local data replication and synchronization strategy for restoring the complete system (both data and application software) within the Consortium's operating environment (i.e., data center replication with the Consortium)?

3.3A.3.5 Identify the disaster recovery timeline.

3.3A.3.6 Identify whether the synchronization of backup data is real-time.

3.3A.3.7 Describe the System Restoration Plan (including any cost associated) that allows the Consortium to continue to operate the complete system (including application software) in the event of a system failure.

3.3A.4 Upgrades and Expansion

The hardware specifications for the proposed locally-hosted system provided by the vendor must, at initial installation, using data volumes and processing characteristics described in this RFP, operate at no more than thirty-five percent (35%) of capacity (for CPU, memory, and I/O performance). The proposed server specifications must support 5 years of transactions based upon five percent (5%) per year increase to present transaction volumes.

3.3A.5 Concurrent Operation

If the CAD/RMS subsystems share the same database, general queries that span a large number of tables might place undue stress on the database server. In addition, a request that locks a large number of rows on a frequently used table could cause contention issues. These types of situations could affect other requests, overall system throughput, and response times. All application systems must be able to operate concurrently.

Explain the safeguards and design patterns that have been used in the application in order to ensure that a single request could not consume a disproportionate level of server-side resources. The Consortium will expect the Vendor to meet the acceptance requirements specified in Section 5.

If the Vendor cannot meet these requirements, an explanation must be provided that addresses how the performance will not be degraded due to a single service request or transaction.

3.3A.6 Network Operating System and Protocol

A description of the Consortium's network is covered in Section 2. The Vendor must provide a system compatible with the Consortium's network.

3.3B Hosting Environment [For SaaS Proposals]

Beyond their functional capabilities for Vendor-Hosted SaaS solutions, evaluations of the Vendors proposed hosted environment will take place. The following specifications apply to the Vendors SaaS service infrastructure and their ability to meet the needs of the organization.

3.3B.1 Hosting Provider and Infrastructure

3.3B.1.1 Identify the SaaS service hosting provider and data center locations.

3.3B.1.2 Identify the infrastructure (hardware, software, operating system, technology platform) used in hosting services.

3.3B.1.3 Identify the primary location where the Consortium's data would be stored.

3.3B.1.4 If the Vendors' hosting provider utilizes virtualization software, Identify the virtualization software (i.e., VM Ware).

3.3B.1.5 Identify the network bandwidth that can be provided by the Vendor and identify options for dedicated bandwidth.

3.3B.2 Data Security

3.3B.2.1 Identify the Hosting Environment as either dedicated (The Consortium's solution and data will be managed in a system independently – single tenant) or shared (the Consortium's solution and data will be managed in a shared system – multi tenant) environment.

3.3B.2.2 If the Vendor operates in a multi-tenant Hosting Environment, identify how the Consortium's data is separated from other solutions.

3.3B.2.3 If the Vendor operates in a multi-tenant Hosting Environment, identify what controls are in place to manage the security of the group's data.

3.3B.2.4 The Vendor shall have administrative, physical, and technical safeguards in place to make the hosting environment HIPAA and CJIS compliant.

3.3B.2.5 Provide the data ownership policy.

3.3B.2.6 Once the service is initiated, the Vendor will identify if the data can be encrypted, what encryption schemes are used, Vendor decryption plan, and encryption testing plan.

3.3B.2.7 The Vendor will perform comprehensive, independent third-party audits as part of their data privacy and information security program and provide such audit findings to the Consortium when service is initiated.

3.3B.2.8 The Vendor will provide a web-portal or separate application that allows management to view the following service audit criteria:
- Load Performance – ability to see service utilization and performance during select times.
- User Statistics – ability to view specific user's utilization of services including times utilized and application utilization
- Problem Records – ability to view active, including status, and resolved problems reported to the vendor

3.3B.2.9 Describe the Data Extraction Plan (including format and any cost associated) for the return of all Consortium data and the expungement of data from the Vendor's systems, in the event of service termination.

3.3B.3 Disaster Recovery Management

3.3B.3.1 Identify your business continuity and disaster recovery options, with their respective costs.

3.3B.3.2 Identify how and where the disaster recovery data is stored.

3.3B.3.3 Describe the replication and synchronization strategy for restoring the complete system (both data and application software) within the Vendors operating environment (i.e., data center replication).

3.3B.3.5 Identify the disaster recovery timeline.

3.3B.3.6 Identify whether the synchronization of backup data is real-time.

3.3B.3.7 If the primary hosting environment is down, the Vendor will enable an active environment which is capable of sustaining Consortium operations until primary hosting environment is functional and secure.

3.3B.4 Identity Management

3.3B.4.1 Describe the identity management solution, including access levels and their respective user rights.

3.3B.4.2 Describe the solution's ability to support Single Sign-On (SSO) and other authorization capabilities (i.e., SAML, HTTP-Fed, Open Auth.) within the identity management solution.

3.3B.4.3 Describe the solution's ability to integrate with the existing identity management solutions (i.e., Active Directory) utilized by the member agencies.

3.3B.4.4 Identify what other user security, authentication, and authorization options are available.

3.3B.5 Standards, Policies, and Regulatory Compliance

3.3B.5.1 Describe Vendor technology standards, policies, and procedures.

3.3B.5.2 Does the Vendor utilize certified PMP project managers for the implementation of their systems?

3.3B.5.3 Describe the solution's compliance with current CJIS requirements and explain how compliance is enforced.

3.3B.5.4 Describe how the Vendor provides encryption and what standards are used (e.g., FIPS 197, FIPS 140-2). Does this affect performance?

3.3B.5.5 Does the solution support current SSAE 16 reporting standards?

3.3B.5.6 Provide audit reports of the Consortium's solution usage and records on a regular basis.

3.4   Integration Services

3.4.1   System Integration

Vendors shall identify the hardware specifications, software, databases, licensing, and connectivity required to support the Statement of Work, end-users, and administrators for the following environments:

- Production
- Training
- Test
- Development

3.4.1A On-Premise Solution Services

The Vendor is to provide design services as follows:

- Recommended specifications or requirements for:
  - Server configurations
  - Storage – Specify requirements for expansion of the Consortium's existing Enterprise Storage based on projected system storage requirements over the next 5 years. The Consortium will acquire any additional storage required.
  - Disaster Recovery Solution – Engineer and design the system's disaster recovery option utilizing either on-site VM and/or a Cloud-based solution.
- Recommendations for any Wide Area Network (WAN) and reconfiguration enhancements to be implemented;
- Work with the IT Department to effect the necessary changes to the member agencies Active Directory to integrate the Vendor provided systems;
- Configuration of all application software at all servers. Deployment includes development and integration of interfaces to key external databases;
- Perform needed file conversion activities (as previously defined);
- Describe what types of APIs and web-services, if any, are available to utilize in pushing data to and from the solution, descriptions of API security and encryption, and limitations the hosting environment places on access to APIs;
- Detailed training of IT administrative personnel and network administrators in the use and operation of the server hardware management systems and tools;
- Detailed training for application software as specified in Section 6.8.

3.4.1B Vendor-Hosted SaaS Solution Services

The Vendor is to provide design services as follows:

- Describe what types of APIs and web-services are available to utilize in pushing data to and from the solution, descriptions of API security and encryption, and limitations the hosting environment places on access to APIs;
- Describe the customization capabilities of the system components within the hosting environment, including: URL naming options, system layout (i.e., header, footer, and login page), workflow, data fields, and customer triggers or organization logic (i.e., incident reports automatically routing to supervisors for review);
- Describe how the system will operate, or not operate, should internet connectivity be lost;
- Recommendations for any WAN network enhancements required to maintain SaaS response time performance;
- Work with the IT Department to effect the necessary changes to the member agencies Active Directory for integration with other systems;

- Configuration of application software including development and integration of interfaces to key external databases;

- Perform needed file conversion activities (as previously defined);

- Detailed training of IT administrative personnel and network administrators in the use and operation of the server hardware management systems and tools;

- Detailed training for application software as specified in Section 6.8.

3.5 Reliability Requirements

The following specification describes the uptime requirements for Vendor's Services following the Consortium's formal acceptance of the Services and throughout the life of the contract between the Consortium and the Vendor.

3.5.1 Processes and remedies in place that support that the system will be available to authorized users for normal use 99.99% of the Scheduled Uptime.

3.6 Performance Requirements

The following specification describes the performance requirements for Vendor's services following the Consortium's formal acceptance of the Services and throughout the life of the contract between the Consortium and the Vendor.

3.6.1 Processes and remedies in place that the system transactions have a response time of 5 seconds or less for the full duration of the Scheduled Uptime.

3.7 End User Equipment

3.7.1 Desktop Workstations

The Consortium utilizes Microsoft Windows 10 on its workstations. Vendor must verify that their products will operate on Windows 10 operating systems and provide an explanation of their roadmap if there are any plans to support HTML5.

3.7.2 Bar Coding

Provide specifications for compatible bar code printers and handheld readers for inventory tracking. These will be purchased by the Consortium at a later time.

3.7.3 Scanners

Provide specifications for scanners that are compatible with your system and capable of simultaneously scanning documents and reading bar codes including:

- 8 ½ x 11-inch single workstation scanners
- 8 ½ x 11-inch high speed batch scanners
- Large form factor (minimum 36 x 48 inch) scanners.

3.7.4 Field Automation Equipment

The Consortium will provide any tools required for field automation. The Vendor will specify recommended hardware and operating system required to run any of their field application(s).

4.0 SERVICE AND MAINTENANCE REQUIREMENTS

4.1 Vendor Instructions

This RFP Section contains general and specific requirements related to the provision of system maintenance and repair and other services throughout the life of the contract between the Consortium and the Vendor. Services described are both warranty and non-warranty services for any equipment and software whose warranty or maintenance is provided by the Vendor.

4.2 General Maintenance Provisions

The following requirements are applicable to maintenance and repair services supplied by the Vendor or Vendor's sub-vendors. Respond to sections corresponding to the proposed solution type (On-Premise and/or Vendor-Hosted SaaS).

4.2A On-Premise Maintenance Provisions

4.2A.1 The proposed system must include a minimum first year maintenance after acceptance, assure availability and fixed price for 5 years of support and maintenance.

4.2A.2 The Consortium may purchase one or more additional years of support and maintenance, and other specified ongoing services, on a year-by-year basis, or purchase a five-year support agreement.

4.2A.3 The production environment must be designed for 24-hour per day and 7-day per week (24x7) high availability with load tolerance and real-time failover. Maintenance must not disrupt service.

4.2B Vendor-Hosted SaaS Maintenance Provisions

4.2B.1 Assure availability for support and maintenance of application software and hosting services.

4.2B.2 The Consortium may purchase one or more additional years of support and maintenance, and other specified ongoing services, on a year-by-year basis.

4.2B.3 The production environment must be designed for 24-hour per day and 7-day per week (24x7) high availability with load tolerance and real-time failover. Maintenance must not disrupt service.

4.2B.4 The Consortium expects the Vendor to provide a sample Service Level Agreement (SLA) of similar scope to the Consortium.

4.2B.4.1 Provide standard policy for remedies associated with Service Level Agreement violations (i.e., uptime and response time)**.**

4.2B.4.2 Verify that that you comply with industry standards ISO 27001, SOC 2 (auditing) and GPDR (data protection and privacy).

4.3   Updates & Enhancements

The following requirements are applicable to all maintenance and repair services supplied by the Vendor and Vendor's sub-vendors.

4.3.1   Operating and Database Software updates for enhancements, and refinements to purchased capabilities will be provided by the Vendor as part of the maintenance.

4.3.2   Vendor will allow for the submission for any system modifications required by the Consortium after system cutover. The vendor shall provide feedback to the Consortium in the form of a price proposal, or the planned development cycle for the change request.

4.3.3   The vendor is to provide the Consortium with their stated update strategy, timeline (i.e., updates annually, bi-annually, etc.), and their requirements for the Consortium to accept such updates.

4.3.4   The Consortium will not be required to upgrade the overall system more than twice per year.

4.3.5   Vendor will provide software and other materials and expenses necessary to maintain the application software system in good operating condition as part of the price for maintenance, for those years in which maintenance is purchased from the Vendor, in conformance with the application specifications and performance requirements stated in this RFP. The Vendor will notify the Consortium prior to making updates or changes to the system.

4.4   System Maintenance

The following requirements are applicable to all maintenance and repair services supplied by Vendor or Vendors sub-vendors.

4.4.1   The entire system solution as proposed in this RFP must include all first-year maintenance costs (for Vendor-supplied software) to conform with contractually agreed specifications, and to protect against any defects or damage, caused by Manufacturer, Vendor, or Vendor's sub-Vendors, in the system's software, as well as offering a 5-year support agreement.

> a). 7 x 24 Maintenance to be provided as part of year one maintenance.

4.4.2   The year one maintenance will begin (for products accepted in phases) at the point that the System is officially accepted by the Consortium, as defined in RFP Section 5.3, System Acceptance.

4.4.3   All software resolutions made under maintenance will be at the sole expense of the Vendor including labor, travel expenses, meals, lodging and any other costs associated with resolution.

4.5   Support Requirements

The following specification describes the support requirements for Vendor's Services following the Consortium's formal acceptance of the Services and throughout the life of the contract between the Consortium and the Vendor.

4.5.1   Provide telephone and email support ("Technical Support") 24 hours per day, 7 days per week, and 365 days per year. Support will include any research and resolution activity performed by Vendor.

4.5.2   Client will access support by calling or emailing the Vendor's Technical Support staff or by submitting a request via the Vendor's customer service web portal.

4.5.2.1 Incident Resolution Process

The Consortium needs to understand the typical process that will be followed by the vendor in order to troubleshoot a user support call. Provide the location of your primary support center, trouble ticket system used, incident analysis tools used (i.e., SolarWinds, OpenView) and what support groups (i.e., application software, database, infrastructure) are involved in the resolution of a support call.

a)   Do the support specialists have direct physical access to the programmers and database managers for incident troubleshooting?

b)   For Vendor-Hosted solutions, do the support specialists have direct physical access to the hosting infrastructure engineers and systems software administrators for incident troubleshooting?

c)   Are the support specialists, programmers, database administrators, systems software administrators and infrastructure engineers all staffed by Vendor employees? If not, what sub-vendors are responsible with each of these areas?

d)   If multiple sub-vendors are involved does the Vendor have defined SLA's with them?

4.5.3   The Vendor will adhere to the following Problem Severity Levels:

- Problem Severity 1

    o   Description: This Problem Severity Level is associated with: (a) The services or system, as a whole, are non-functional or are not accessible; (b) unauthorized exposure of all or part of the Consortium's data; (c) loss or corruption of all or part of the Consortium's data.

    o   Request Response Time: 30 minutes.

    o   Request Resolution Time: 2 hours.

- Problem Severity 2

    o   Description: This Problem Severity Level is associated with significant and / or ongoing interruption of a User's use of a critical function (as determined by the User) of the system/services and for which no acceptable (as determined by the User) work-around is available.

    o   Request Response Time: 1 hour.

    o   Request Resolution Time: 4 hours.

- Problem Severity 3

    - Description: This Problem Severity Level is associated with: (a) minor and / or limited interruption of a User's use of a non-critical function (as determined by the Authorized User) of the Services; or, (b) problems which are not included in Problem Severity Levels 1 or 2.

    - Request Response Time: 8 hours.

    - Request Resolution Time: 24 hours.

- Problem Severity 4

    - Description: This Problem Severity Level is associated with: (a) general questions pertaining to the system/services; or, (b) problems which are not included in Problem Severity Levels 1, 2, or 3.

    - Request Response Time: 8 hours.

    - Request Resolution Time: 48 hours.

4.5.4   In the event that a problem resolution is not met within the Request Resolution Time, the Vendor will adhere to the following protocol:

- If a Problem Severity Level 1 or 2 request cannot be corrected to the reasonable satisfaction of the requestor within the Request Resolution Time after the requestor makes the initial request for Technical Support, Vendor will: (a) immediately escalate the request to Vendor's management; (b) take and continue to take the actions which will most expeditiously resolve the request; (c) provide a hourly report to the requestor of the steps taken and to be taken to resolve the request, the progress to correct, and the estimated time of correction until the request is resolved; and, (d) every four (4) hours, provide increasing levels of technical expertise and Vendor management involvement in finding a solution to the request until it has been resolved.

- If a Problem Severity Level 3 or 4 request cannot be corrected to the reasonable satisfaction of the requestor within the Request Resolution Time after the requestor makes the initial request for Technical Support, at the sole election of requestor: (a) Vendor will work continuously to resolve the request; or, (b) requestor and Vendor will mutually agree upon a schedule within which to resolve the request.

5.0 PERFORMANCE REQUIREMENTS

5.1 Vendor Instructions

This RFP Section contains general and specific requirements related to the performance of the proposed system, both at the point of system acceptance and throughout the life of the contract between the Consortium and the Vendor.

System Acceptance will occur in phases as various milestones identified in the implementation plan and agreed to by the Consortium are reached. The Vendors implementation plan must clearly define the hardware and software deliverables, tasks or other criteria associated with each milestone.

5.2 Testing

5.2.1 A sample test plan will be provided with each proposal. The successful Vendor must, as one of the early milestones, submit an acceptance test plan for the Consortium's approval. The test plan must document how each of the functional specifications are to be tested, the method of verifying the results, and the expected results. The test plan must also include a scenario test that allows for the System (integrated hardware/software) to operate under a simulated test situation.

5.2.2 The performance requirements specified in this RFP must be met before the system is accepted. Vendor is to specify any requirements it has for performance testing.

5.2.3 The Vendor must prepare a plan for correcting failures in any part of the system. Said plan must include reasonable remedies for the Consortium to exercise if failures are not corrected in a timely manner.

5.3 System Acceptance

The following specifications apply to the requirements for the Consortium's acceptance of the Vendor's system after phase in begins.

5.3.1 The Consortium expects the starting date for the project to be immediately following the execution of the contract.

5.3.2 Beginning with the first day after the completion of each phase (phases will be specified in the implementation plan) that the proposed system phase is operational and available to the Consortium for testing; an acceptance test will be conducted for thirty consecutive calendar days (the Acceptance Period).

5.3.3 During the Acceptance Period, the proposed system will undergo a live test that confirms the configuration, data conversion, performance and reliability requirements using the mix of users, applications, and functions as described in this RFP.

6.0 IMPLEMENTATION REQUIREMENTS

6.1 Vendor Instructions

RFP Section 6 contains all general and specific requirements related to the period between site planning and our final acceptance of the system. RFP Section 6.10 contains a list of required contents for your implementation plan.

6.2 General Implementation Requirements

6.2.1 Conduct of Work

All work will be conducted in a professional and orderly manner. Installation must be completed in a skillful manner.

6.2.2 Use of Facilities

Reasonable office facilities will be provided based upon stated requirements of the Vendor. Access to any area outside of normal business hours is restricted; necessary access must be arranged each day as needed with the Consortium's Project Manager.

6.2.3 Qualifications of Implementation Staff

Vendor implementation staff must be fully trained and certified by the manufacturer(s) of the system(s) you propose. Their training must be up-to-date for the specific systems being installed. In addition, all key implementation staff must be experienced in similar prior installations of the system(s).

Additional requirements include:

- Submission of qualifications by Vendor and approval of all key staff members by the Consortium prior to project start
- Maintaining the involvement of Vendor's personnel is essential to the project throughout the life of the project, up to and including training, implementation and acceptance
- Timely replacing any staff deemed unqualified by the Consortium
- Directing staff to comply with City rules and regulations
- Staff may be subject to a security check.

Vendor must be CJIS certified. Documentation to be provided includes:

- The Vendor's management security control agreement
- A list of all persons working on the project to ensure each has necessary CJIS background check and associated training.

6.2.4 Documentation

6.2.4.1 General

a. If selected, the Vendor must be able to supply comprehensive hard and soft copy documentation for the system which covers at least the following subjects:

    i) Systems Administration and Management (user privileges, access and security administration, etc.) integrated with Microsoft Active Directory.

    ii) Utilities and tools to monitor resource utilization

    iii) Web development tool kit, including API's

    iv) System wide Entity Relationship Diagram (ERD) with documentation

    v) Toolkit manuals

    vi) Report generation scripts/Change Control tools

    vii) Legacy Data Migration (Extract, Transfer, Load – ETL).

b. The system documentation must be consistent with the instructions supplied by the internal help systems for the application.

    i) The system must include no less than four original copies of documentation describing the use of the system, and its administration. The Consortium requires authority to copy documentation for internal use.

    ii) Strong preference to support internal, context sensitive, help which is granular enough to provide help to specific items on the screen without having to scroll through a help file to find the description of the item.

    iii) The Vendor must provide a printed database schematic and data dictionaries to assist the customer with the addition of site-specific fields and support for the system. Electronic copy to be provided.

6.2.4.2 Software Documentation

The proposal must include a list and description of the software that is required to operate the proposed hardware/software configuration. Once selected the vendor must provide documentation. Examples of these are:

- Application System Reference
- Application System Tutorial.

The Consortium requires that the Vendor provide documentation (1) electronic copy for any software that the Vendor supplies as part of the system configuration.

6.2.4.3 System Implementation Documentation

Prior to commencing work, the Vendor must provide documentation to include systems design for Vendor installed components, with clearly identified interface points to other systems, Implementation Plan, System Test Plan and Procedures, and Training Plan. The delivery of these and certain key documents are expected to be indicated as milestone points on the Work Breakdowns Structure (WBS) of a Microsoft Project Schedule, which will be provided by the Vendor as their first deliverable.

6.2.4.4 Training and Operations Documentation

Several documents will be prepared that will be used in training personnel and/or in operating the system. The Vendor must describe these documents in its proposal and specify the number of each that will be delivered to the Consortium.

6.3 Project Management

The Consortium will have a project manager for this implementation project. The Consortium's Project Manager will be the point of contact with the Vendor's project manager in all areas indicated in this RFP section. He/she will be empowered to resolve disputes and make decisions about any changes to the implementation plan or technical aspects of the system. He/she will also provide liaison with agency department heads, and will assist in coordinating work with the Vendor.

The Vendor must also name a project manager. Key expectations for this individual include that this person:

- Will be empowered to authorize project changes.

- Will provide periodic written status reports at a mutually agreed upon time frame.

- Will maintain the involvement of the same Project Manager throughout the entire project and through implementation.

Subsequent to selection, the Vendor will present the project manager to Consortium management for the Consortium's approval.

6.3.1 Coordination

Vendors must include a review of the project plan in each weekly teleconference briefing, and monthly on-site meeting, or more often if necessary. This briefing must include a review of the tasks accomplished and items delivered or installed. The Vendors Project Manager must keep the Consortium's Project Manager fully informed of any change in schedule and must provide a modified project plan including Gantt Chart for each schedule change of more than one day.

Vendors must deliver written notice to the Consortium no less than two weeks prior to the completion of each milestone. The purpose of this notice must be to allow the Consortium to schedule personnel who may be required to participate in testing or other activities associated with a pending milestone.

6.3.2 Scheduling

6.3.2.1   All proposals must include a preliminary schedule for the complete implementation of the proposed system components where the expected order of deployment is:

- Computer Aided Dispatch
  - Call Taker
  - Dispatch
  - Administration

- Fire
- CAD Mobile
- Records Management System
  - Case/Records Management
  - Property
  - Warrants
  - Field Reporting
  - Civil Process
  - Crime Analysis
- Detention Management System
  - Booking
  - Identification
  - Detainee Property

6.3.2.2 The preliminary proposal schedules must include clearly identified milestones and tasks for each of the major activities and events that are planned for completion of the System through the complete system acceptance.

6.3.2.3 The Vendor (or Vendors) must be required to finalize a detailed schedule and Implementation Plan, for approval by the Consortium, as part of the contract negotiation process.

6.3.2.4 The detailed schedules must be included as part of the Contract, and must be maintained by the Vendor (or Vendors), and must be updated and reviewed with the Consortium at regular intervals as part of normal project management functions by the Vendor.

6.3.2.5 All scheduled changes are subject to the prior approval of the Consortium.

6.3.2.6 Coordination with the Consortium's project manager is required. The Consortium will not be responsible for any extra costs in the implementation phase that are caused by failure on the Vendors part to coordinate with the project manager.

6.3.2.7 Installation of the main system components must also be coordinated with the Consortium's project manager. Specify what specific interactions will be required, and what time will be required to make any required interfaces.

6.3.2.8 Installation of user equipment in occupied areas must minimize disruption to normal business activities. Specify how this requirement will be met.

6.3.2.9 Implementation of application systems must follow a logical progression, with testing and acceptance of predecessor systems prior to the implementation of additional systems.

6.3.2.10 During testing and startup of the new systems, on-site Vendor technical support is required.

6.4 Site Planning

The Vendor, as part of a walkthrough scheduled with the Consortium after award, will verify the operating environment and recommend the appropriate action for optimal implementation and usage of system by consortium staff.

6.5 Business Process Review

Vendor is required to analyze the workflow for each of the work areas that will be impacted by the new applications in order to determine the appropriate configuration settings for the system.

6.6 Coordination Meetings

Vendor is required to integrate with the Consortium's network environment and other current applications. Coordination meetings will be required to ensure mutual understanding and shared expectations concerning the nature and extent of interface and integration activities. Further, to assure timely compatibility and connectivity, the schedule as preliminarily detailed below, must be accommodated.

6.7 Phase-in Requirements

Project schedule expectations are provided below.

6.6.1 Vendor is required to analyze the workflow for each of the work areas that will be impacted by the new applications in order to determine the appropriate configuration settings for the system.

6.6.2 All system components must be tested and the results of testing presented to the Consortium project manager per Section 5.

6.6.3 A Phase-in plan is required as part of your implementation plan, covering testing, and the sequence and timing of events.

6.6.4 Vendors must have their own personnel at the Consortium site during testing and start-up ("go live") periods in order to ensure a smooth phase in process.

6.8 Data Migration

Migration of present data files is required. It is expected that the conversion programs will be thoroughly tested, and that full data sets will be totally converted and loaded into the system during an evening or weekend. Provide the programs/scripts used for scrubbing data (i.e., addresses) prior to data migration. Provide information on the methodology used to ensure all data was properly migrated. Provide information on vendor team utilized for conversion with their experience converting for similarly sized agencies. Use the **Proposal Response Forms, Section 6** to supply this information.

6.9   Training

6.9.1   Training Guidelines

The general training approach desired will be training of System Administrators and support personnel for general systems administration and operations, and select staff for application operations. The Vendors training programs must be designed and conducted to provide complete familiarization in applicable system operation.

The Vendor must describe the types of training classes that will be conducted, the number of persons that can be trained in each session, and the total number of hours required for each person to be trained. The training plan must provide for rotating shift operations.

All training, insofar as possible, is to be conducted on-site in Consortium facilities. A copy of all training materials used by the Vendor is to be delivered to the Consortium upon conclusion of the training. The Consortium has a computer training lab onsite with multiple student workstations and 1 instructor workstation.

6.9.2   System Training and Documentation Requirements

The minimum training requirements are outlined at the end of this Section. The Vendor should use this as a guideline of requirements and should comment on suggested training.

6.9.3   Training Schedule

With the Implementation Plan, the Vendor must submit a schedule of all proposed training modules with the following information:

- Course summary/outline
- Duration of training for each module
- Maximum class size
- Audience
- Location of training
- Student prerequisites.

6.9.4   Training Environment

- The system shall include a training environment that provides the real system and allows users to access training databases.
- Users logged on to the training database must utilize the same commands, forms and system features as users logged on to the live system.
- No data entered or command invoked while logged to the training database must corrupt the live system or noticeably impede the performance of the live system.

6.9.5   Training Volumes

Training proposals must provide for System Administration, Application Software and Report Generation, primarily through on-site training. Additional Vendor classroom training may be proposed. The training requirements are shown on the next page.

Training Requirements		
Class	**Total Trainees**	**Training Method**
▪ System Administration	10	Onsite
▪ CAD System	10-20	Onsite
▪ Records Management System	10-15	Train-the-Trainer
▪ CAD Mobile / FBR	20-25	Train-the-Trainer
▪ Property and Evidence	10	Onsite
▪ Detention Management System	5-10	Train-the-Trainer
▪ Ad Hoc Report Generation	20 - 30	Onsite

6.9.6 Ongoing Training

The following requirements are applicable to the provision by Vendor of various categories of training after Implementation and Acceptance:

▪ Train-the-Trainer capability to be provided with the above.

▪ Vendor is asked to describe their program for follow-up training, if and when needed. This training is a separately chargeable item.

▪ Rates for subsequent years are subject to negotiation.

▪ Vendor may make training available at both Vendors' training facility and, at the Consortium's option, at the Consortium's site.

▪ Charges for training must be included in Price Proposal Sheet.

6.10 Implementation Plan

Your response to these implementation requirements should be included in the implementation plan. This plan can be in your format, but it must:

a. Include a complete schedule of events, consistent with Section 6.6, in narrative and GANTT chart form.

b. Show an implementation schedule that has specifically designated phases; each phase should have its acceptance plan and milestones. The overall implementation plan should combine all phases into a coherent plan.

c. Respond to all of the requirements in this RFP section in the narrative using the same numbering scheme as shown in this RFP. State how each requirement will be met.

d. Be able to be used as a stand-alone document for use by the project managers and implementation staff.

e. Incorporate training on Preventative Maintenance procedures and software, if offered (please describe).

7.0 CONTRACT REQUIREMENTS

7.1 Instructions

7.1.1 The following contractual terms, contained in Section 7, are required. These instructions apply to all quotations or bid submittals and become a part of terms and conditions of any bid packet submitted. Note any exceptions taken to this section in the **Proposal Response Forms, Section 7**.

7.2 Terms

7.2.1 Refer to Attachment A4 - Consortium Terms and Conditions

8.0 PRICE REQUIREMENTS

8.1 General Information

8.1.1 Important Notice

Please provide your Price Proposal. Vendor shall identify the software and services required to support their Statement of Work.

8.1.2 Price Proposal Format

The price proposal response forms provide specified areas for either On-Premise or Vendor-Hosted SaaS solutions. Vendors are to respond to either section in accordance to their proposed solution. If the Vendor is proposing both solutions, complete two separate price proposals, one for On-Premise and one for Vendor-Hosted.

Submit your price proposal exactly as listed below:

- A summary price proposal, for each option being offered, either on the sheet provided or a comparable form. See RFP Section 8.2 below.

- A set of supporting price details, on the sheets provided or comparable form. See RFP Section 8.3 below.

- Explanatory notes further clarifying how you derived the prices in your proposal, listed on or attached to the supporting price detail sheet.

- A strong preference exists for a software site license to be provided to the Consortium. Explain limitations if otherwise.

- You may also add any further narrative as needed to describe your price proposal.

8.1.3 Evaluation Period

Our price evaluation will use a uniform method for all proposals. The method will be a 5-year life cycle net present value (NPV) analysis using uniform assumptions for economic analysis. We will also consider Vendor supporting price details in the context of the related sections of your functional proposal.

Time for Consideration: Vendor warrants by virtue of submitting the proposal that costs as outlined in his proposal will be good for an evaluation period of two hundred seventy (270) calendar days from the date of proposal opening. *Vendors will not be allowed to withdraw or modify their proposals after the opening time and date.*

8.2 Summary Price Proposal

- The attached summary price sheet is clearly marked.

- Complete the sheet as instructed. Use duplicate or additional sheets as necessary.

- Add explanatory notes as required for clarity.

8.3   Supporting Price Detail

8.3.1   Response Sheets

In addition to the price summary, there are several supporting price detail sheets, in Section Eight, Price Proposal, of the **Proposal Response Forms**; each supporting price detail sheet corresponds to major lines on the Summary Price Proposal. Complete all sheets as instructed on the form. Use duplicate or additional sheets as necessary, but do not change the formats. Add explanatory notes as required for clarity.