



Texas Department of Public Safety  
5805 North Lamar Blvd.  
Austin, TX 78752  
Phone: 512-424-2870  
Fax: 512-424-5419  
Email: [alfred.ramos@txdps.state.tx.us](mailto:alfred.ramos@txdps.state.tx.us)  
TXDPS Purchaser: Alfred Ramos, CTPM

---

**Request for Offer (RFO)  
For  
Crime Records Service  
Remotely Hosted  
Criminal Incident Records  
Management System  
Project**

RFO Number: 405-IT10-0542  
RFO Closing Date: 06-16-2010  
RFO Closing Time: 3:00 pm

**Class-Item:**

**915-51; 920-40; 920-48; 956-35; 962-95**

## Table of Contents

Section 1: Background	1
Section 2: Introduction	1
Section 3: General Information	2
Section 4: Questions, Responses and Vendor Conference	7
Section 5: Offer Submission Requirements	7
Section 6: Additional Requirements	13
Section 7: Purchasing Information	15
Section 8: RMS Specifications	16
Section 9: JMS Specifications	23
Section 10: CAD Specifications	29
Section 11: Software and Hardware	34
Section 12: System Functionality	35
Section 13: Software Licenses	36
Section 14: RRMS Modifications and Enhancements	36
Section 15: Evaluation Criteria	37
Section 16: Attached Contract	37
Section 17: Contract Term	38
Section 18: Appendices	38

## **1 BACKGROUND**

Many local Texas Law Enforcement Agencies (LEA) do not have the resources required, neither financial nor technical, to establish and maintain a records management system to store incident and related data generated within its jurisdiction. The Texas Department of Public Safety (TXDPS) Remotely Hosted Criminal Incident Records Management System (RRMS) Project is intended to provide a remotely hosted records management system (RMS), jail management system (JMS) and/or computer aided dispatch (CAD) local LEAs can access as services (coupled or stand alone) provided by the successful vendor(s). The RRMS will provide the local LEAs with a virtual database that they will be able to remotely access on a 24x7 basis in a manner that is consistent with the security requirements articulated in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy.

The Vendor will provide for, at minimum, the database structure to capture data elements required by Chapter 60 Texas Code of Criminal Procedure as well as substantial subset of the data elements defined in National Data Exchange (N-DEX) Information Exchange Package Documentation (IEPD) current version for an Incident Report, an Arrest Report, or a Service Call Report.

The capture of additional data elements needed to map to N-DEX IEPDs associated with Missing Persons Reports and Suspicious Activity Reports will be considered as value added for the RRMS.

The successful Vendor(s) will also provide technical support for the local user as it applies to the setup and use of the RRMS service.

## **2 INTRODUCTION**

### **2.1 Scope**

The RRMS Project encompasses the implementation of a new service that will provide a remotely hosted database service for local LEAs to enter, query and export incident and related data. The scope of this project is a deliverables-based, turnkey solution which includes:

- 2.1.1** Design, development, and implementation of an electronic system that meets the requirements of this Request for Offer (RFO). Programming and database design methodologies must ensure that existing and future business requirements can be incorporated in a timely manner
- 2.1.2** Migration of legacy local LEAs RMS, JMS and/or CAD data (where applicable) into the new application
- 2.1.3** Identify, recommend or supply the minimum technical hardware specifications required to host
- 2.1.4** Identify and recommend the minimum technical hardware specifications necessary to access the system

- 2.1.5 Provide an effective interface for the export of incident data into the N-DEx IEPD version v. 2.0.0 [Based on NIEM 2.0 and LEXS 3.1.1], available at: [http://it.ojp.gov/jsr/common/viewDetail.jsp?sub\\_id=258&view=yes&keyword=1](http://it.ojp.gov/jsr/common/viewDetail.jsp?sub_id=258&view=yes&keyword=1)
- 2.1.6 Identifying and implementing a telecommunication methodology that is compliant with the FBI CJIS Security Policy
- 2.1.7 Application, hardware (as applicable) and/or user support
- 2.1.8 Project Management responsibilities

## 2.2 Objectives

The primary objectives of RRMS are receipt, storage, and sharing of essential criminal information related to incident data generated by the participating local LEAs. Incident data is defined as all of the events that are associated with a law enforcement incident cycle.

The goal of RRMS is to improve the effectiveness of the criminal justice community by providing for the timely exchange of documented and reliable information through use of a system that affords the tools necessary to efficiently collect, evaluate, organize, analyze, and disseminate incident and related data.

In order to provide the best value for the participating agencies, TXDPS will develop a list of one or more Vendors (Certified Provider) whose Offer(s) is/are evaluated as the top solution(s) in response to this RFO. Local LEAs will be allowed to select a Certified Provider that provides the best service and product for that agency's implementation of RRMS. While the receipt, storage, and sharing of incident data is the primary goal of the RRMS, Vendors are encouraged to demonstrate their ability to capture additional data elements specifically associated with the arrest information required by Chapter 60 of the Texas Code of Criminal Procedure for reporting to the state as well as data elements associated with suspicious activity reports and Missing Person Reports.

## 2.3 Stakeholders

Many local Texas LEAs lack the necessary resources to effectively collect or share criminal incident data and will be the primary customers of this service. Offers must include scalable factors effecting costs to allow TXDPS and the local LEAs customer(s) selection of the most cost effective solution which meets their needs. LEAs are scaled according the following dimensions for the purpose of this RFO:

Quantity of Users:

Size 1 =  $\geq 51$

Size 2 = 26 to 50

Size 3 = 11 to 25

Size 4 =  $\leq 10$

## 3 GENERAL INFORMATION

### 3.1 Project Management

TXDPS and the Certified Provider(s) will be required to identify a single point of contact as the assigned Project Manager (PM).

### 3.2 Schedule of Events

RFO Solicitation Released	05-19-2010
Deadline for submission of Non-Disclosure	06-04-2010, 3:00 pm
Vendor Conference	06-07-2010, 2:00pm
Deadline for submission of questions	06-07-2010, 5:00 pm
Posting of responses to questions	06-10-2010, 5:00 pm
<b>Deadline for submission of Offers</b>	<b>06-16-2010, 3:00 pm</b>

Offer evaluation and scoring, contract negotiations and award will directly follow Offer submission.

### 3.3 Revisions to Schedule

TXDPS reserves the right to change the dates in the schedule of events for this RFO with posted addenda.

### 3.4 Offer Binding for 90 Days

Vendor's entire Offer is binding upon Vendor for 90 days from Offer submission date.

### 3.5 Revisions

Offer cannot be altered or amended after submission date and time. Alterations made prior to submission date and time should be initialed by Vendor or their authorized agent. No Offer may be withdrawn after submission date and time without approval by TXDPS.

### 3.6 Award and Cancellation of RFO

TXDPS reserves the right to accept or reject all or any part of an Offer, waive minor technicalities and award the Offer to best serve the interest of the State. TXDPS also reserves the right to cancel this RFO or any portion of this RFO at any time.

### 3.7 Delivery

Unrealistic delivery timeline projections may cause the Offer to be rejected.

### 3.8 Tax Exempt

Purchases for State use are exempt from State Sales Tax and Federal Excise Tax. Do not include tax in Offer. Excise Tax Exemption Certificates are available upon request.

### 3.9 Definitions

Where any word or phrase defined below, or a pronoun used in place thereof is used in any part of this RFO, it shall have the meaning herein set forth.

#### Automated Fingerprint Identification System (AFIS)

The TXDPS database designed to process and store fingerprint submissions. AFIS is the tool utilized by TXDPS to determine positive identification of individuals based upon fingerprints.

Agreement

A written agreement and fully executed document in which a Vendor agrees to provide goods or services in accordance with the established price, terms and conditions. Term interchangeable with Contract.

Certified Provider

A Vendor whose Offer(s) was evaluated and selected as qualified to provide RRMS service to Texas law enforcement agencies.

Change Management (CM)

Change Management is the process of planning, communicating, coordinating, and implementing changes successfully. The purpose of CM is to ensure that changes to the information systems environment are consistently made with minimum disruption to service levels.

CJIS Security Addendum

Document that describes the TXDPS security related requirements that apply to all vendors that work on this project. An executed copy of the CJIS security addendum is a required part of the contract.

Computer Aided Dispatch (CAD)

An automated law enforcement system which provides for the storage, retrieval, retention, manipulation, archiving, and viewing of dispatch information, records, documents, or files related to operations such as resource management, call taking, location verification, dispatching, unit status management, and call disposition.

Contract

Term interchangeable with Agreement.

Contractor

Individual, partnership, corporation, business association, trust, joint-stock company, education institution, or other entity awarded the contract. Interchangeable with Vendor.

Criminal Justice Information Services (CJIS)

Criminal Justice Information Services Division of the FBI. The CJIS Division was established in February 1992 to serve as the focal point and central repository for criminal justice information services in the FBI. The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice community.

Electronic State Business Daily (ESBD)

Texas Comptroller of Public Accountants e-Services posting of procurement opportunities and awards for services or goods over \$25,000.

Electronic Biometric Transmission Specification (EBTS)

The EBTS defines requirements that agencies must adhere to when electronically communicating with the FBI's IAFIS.

*Federal Bureau of Investigation (FBI)*

National security organization whose mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal and international agencies and partners.

*Interstate Identification Index (III or "Triple I")*

The III is the national criminal history record information index accessible through the same network as the NCIC.

*Information Exchange Package Documentation (IEPD)*

Information Exchange Package Documentation is a set of data artifacts used to support the sharing of data for a particular business purpose. It is a set of documentation that accurately and completely defines the contents of a specific information exchange.

*Integrated Automated Fingerprint Identification System (IAFIS)*

IAFIS is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

*Jail Management System (JMS)*

An automated law enforcement system which provides for the storage, retrieval, retention, manipulation, archiving, and viewing of jail information, records, documents, or files related to operations such as processing, management, health care, and disposition of offenders plus administrative functions.

*Law Enforcement Agencies (LEAs)*

Local, state and federal law enforcement agencies and staff including any regional collaboration involved in the administration of criminal justice duties authorized to access CJIS data.

*National Information Exchange Model (NIEM)*

The National Information Exchange Model is a partnership of the U.S. Department of Justice and the Department of Homeland Security. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM will standardize content (actual data exchange standards), provide tools, and managed processes.

*National Crime Information Center (NCIC)*

NCIC is a computerized database of documented criminal justice information containing seven (7) property files contain records for articles, boats, guns, license plates, securities, vehicles, and vehicle and boat parts plus eleven (11) person files are the Convicted Sexual Offender Registry, Foreign Fugitive, Identity Theft, Immigration Violator, Missing Person, Protection Order, Supervised Release, Unidentified Person, U.S. Secret Service Protective, Violent Gang and Terrorist Organization, and Wanted Person Files.

National Data Exchange (N-DEx)

N-DEx is an automated investigative tool that provides law enforcement with the ability to search, link, analyze, and share criminal justice information such as, incident/case reports, incarceration data, and parole/probation data nation-wide.

Project Manager (PM)

Appointee, designee, or alternate designee assigned by both TXDPS and the Vendor/Certified Provider responsible for coordination of the planning, execution and conclusion of the RRMS Project.

Records Management System (RMS)

An automated law enforcement system which provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files related to operations such as incident, arrest, citation, warrant, case management, field contacts and other operational orientated records.

Remotely Hosted Criminal Incident Records Management System (RRMS)

The title of this project is RRMS which encompasses software including RMS, JMS and/or CAD.

Request for Offer (RFO)

All documents, whether attached, posted or incorporated by reference, utilized for soliciting competitive Offers.

Service Level Agreement (SLA)

Document which defines post implementation/production responsibilities and obligations of the Certified Provider, TXDPS and local LEAs.

Texas Department of Public Safety (TXDPS)

State of Texas law enforcement agency.

Suspicious Activity Report (SAR)

Standardized format for the reporting of suspicious activity.

User(s)

LEA customer's personnel, machine or processes.

### **3.10 Grant Funding**

Grant funding may be used in part or in full for the TXDPS RRMS Project. Applicable Grant requirements or obligations will be imposed.

### **3.11 Texas Bidders**

Procurements by state agencies must follow all requirements of Government Code Sec. 2155.444 related to goods or products produced or grown in this state by a Texas bidder that is owned by a service-disabled veteran who is a Texas resident.

## **4 QUESTIONS, RESPONSES AND VENDOR CONFERENCE**

### **4.1 Written Questions**

Questions concerning this RFO will be accepted until deadline for submission of questions (**see Section 3.2 Schedule of Events**) and must include the project name, RFO number and applicable section. Questions specific to this RFO must be submitted by e-mail addressed to TXDPS Purchaser in Appendix B.

### **4.2 Verbal Inquiries**

Verbal Inquiries will not be accepted. Official responses to written questions will be posted on the ESB D Texas Marketplace, as an addendum to the RFO on or before the deadline for the posting of response to questions (**see Section 3.2 Schedule of Events**). The website address is <http://esbd.cpa.state.tx.us>. The State will not be bound by any oral statement or representation contrary to the written specifications of this RFO.

### **4.3 Vendor Conference**

#### **4.3.1 Vendor Conference**

TXDPS will hold a Vendor Conference at the TXDPS Headquarters Complex in Austin, Texas; Criminal Law Enforcement Conference Room (Building E). Conference date and time is provided in **Section 3.2 Schedule of Events**. Map of TXDPS Headquarters Complex may be located at <http://www.txdps.state.tx.us/images/dpslegendmap0209.pdf> Vendors attending the Conference should provide a copy of anticipated questions upon attendance registration. Any questions submitted prior to the Conference will be discussed during the Conference. Questions resulting from the Conference or received prior to the deadline stated in **Section 3.2 Schedule** will be posted together with all responses on the ESB D.

## **5 OFFER SUBMISSION REQUIREMENTS**

### **5.1 Offer Response Submission**

**Offers are required to comply with the instructions outlined in this section.**

Each Offer must be typewritten in black ink, 12 point Arial font, and submitted on paper that is 8.5" x 11", bound in appropriately sized binders and tabbed defining the contents of the sections. Pages shall be numbered consecutively and reflect the total number of pages in the Offer.

### **5.2 Offer Response Delivery Instructions**

Qualified Vendor's are invited to submit an Offer in accordance with the requirements outlined in this section. The Vendor is required to address all aspects of this RFO and must be submitted on time to the address provided in Appendix B.

Offers may be mailed, hand-delivered or courier delivered, but must be physically received by TXDPS as specified in **Section 3.2**. The Vendor must allow sufficient mail handling on or before date and time as specified in **Section 3.2** to ensure timely delivery of the Offer to the submission location. Delivery of responses via United States Postal Service is acceptable; however, due to the internal TXDPS mail processing procedures, this method may cause a delay in delivery to the TXDPS Purchaser. TXDPS will not be responsible for any delays associated with this method of delivery.

No extension of time will be granted for submissions by mail or any other method of submission. Offers submitted by e-mail, facsimile transmission, or any other forms of electronic submission are **not** allowed. Offers received **after** the submission deadline **will** be rejected and returned unopened to the sender.

### 5.3 Offer Response Specifications

Offers must comply with the following standards:

**5.3.1** All packages and boxes must clearly reference the RFO name and number

**5.3.2** The Technical and Cost Offers must be bound separately. For the purposes of this RFO, the **Technical Offer** is defined as the entire Offer in response to this RFO, excluding the Cost Offer

**5.3.3** Vendor must submit one (1) signed original and four (4) additional copies of the Technical Offer and one (1) signed original and four (4) copies of the Cost Offer

**5.3.4** Vendor must submit one (1) electronic copy of the Technical Offer and Cost Offer on CD-ROM. Electronic copies must be formatted using MS Word 2000, or higher, and MS Excel 2000, or higher, software

### 5.4 Offer Submission Checklist

This checklist is provided to aid the Vendor in ensuring a proper Offer is submitted in the required format.

Required Offer Component	Completed (Y/N)
Title Page (Section 5.5)	
Table of Contents (Section 5.6)	
Executive Summary (Section 5.7)	
Vendor Information (Section 5.8/Appendix B)	
Qualifications and References of Vendor (Section 5.9.1 and 5.9.2)	
Criminal Justice Customers (Section 5.9.3)	

<b>Required Offer Component</b>	<b>Completed (Y/N)</b>
Additional Qualifications (Section 5.10)	
Vendor Staff Experience (Section 5.11)	
Signed Anti-Lobbying Affidavit (Section 5.12 /Appendix C)	
Signed Affirmation Clauses and Preferences (Section 5.13/Appendix D)	
Signed HUB Subcontracting Plan (Section 5.14/Appendix E)	
Signed FBI CJIS Security Documents (Section 5.16/Appendix G)	
Contract (Section 5.17/Appendix J)	
Service Level Agreement (Section 5.18/Appendix K)	
Evidence - Accessibility Standards (Section 6.6 Item 2)	
Project Specifications (Sections 8 through 11)	
System Functionality (Section 12)	
Software Licenses (Section 13)	
Cost Offer (Appendix A)	

### **5.5 Title Page**

The Offer title page must include the following information:

- “Project Name”
- RFO ID Number
- Name and address of the Vendor
- Vendor’s State of Texas Taxpayer Number and Federal Employer’s Identification Number

### **5.6 Table of Contents**

The Offer must be submitted with a table of contents that clearly identifies and denotes the location of each section and sub-section of the Offer. Additionally, the table of contents must clearly identify and denote the location of all enclosures and attachments to the Offer including relevant page number(s).

### **5.7 Executive Summary**

The executive summary must be limited to six (6) pages and must provide a concise summarization of the deliverables being proposed to meet the requirements of this solicitation and the Vendor’s approach to providing the deliverables. The executive summary must exclude cost information.

### **5.8 Vendor Information (Appendix B)**

The Vendor must fully complete all required information listed in Appendix B. Name and location of major offices and other facilities that must be used as part of the Vendor's performance under the terms of this RFO must be listed on separate sheets that must follow the submitted Appendix B.

### **5.9 Qualifications and References of Vendor**

The Vendor must provide detailed information to substantiate that it has the experience and qualifications necessary to provide the deliverables requested in this RFO. Specifically, the Vendor must provide:

**5.9.1** An Overview and brief history of the Organization and a description of what uniquely qualifies the organization for this deliverables based contract.

**5.9.2** Offer must identify three (3) past projects with references that are *similar* in scope to the specifications in this RFO. Identified projects must include:

- Project(s) actual start and completion dates (MUST include MM/YYYY)
- Project(s) targeted start and completion date (MUST include MM/YYYY)
- Contact name and telephone number
  - i. Program Manager
  - ii. Project Manager
- Project Overview (Brief description of the deliverables)
- Cost
  - i. Contract
  - ii. Project
- Project Scope
- Project details that reflect similar experience working with systems, procedures or data outlined in Section 5.10 Additional Qualifications

Failing to include all requested information will result in a reduction in score for each deficient project listed. Offers received that identify more than three (3) projects may increase points awarded during the selection process – up to ten (10) points per project similar in scope to the RRMS Project for a maximum of fifty (50) points. TXDPS RFO evaluation team may contact references provided by the Vendor during the evaluation process.

### **5.9.3**

Vendor must provide a complete list of all criminal justice customers in the state of Texas which have an active contract, permit, software license agreement, service level agreement, or rights for any product, software, module, system, application, data warehouse or database which the vendor currently (or has previously) markets, sells, distributes, manufactures, develops, customizes, enhances or provides for use in the administration of criminal justice.

Failure to include a complete list will result in disqualification.

## **5.10 Additional Qualifications of Vendor**

Vendor must sufficiently demonstrate by providing project scope, start/end dates (in MM/YYYY format) and detailed experience in the design, development, and implementation of Gang, Criminal Investigative Systems or Criminal Justice Programs with the following applications, programs, data, interfaces, systems, etc for a minimum of three (3) years or Offer will be disqualified:

**5.10.1 Criminal Justice Interfaces**

**5.10.2 Criminal Justice Databases**

**5.10.3 Criminal Justice Application Documentation**

**5.10.4 XML**

**5.10.5 Local, state or federal law enforcement Record Management System**

Offers received that sufficiently demonstrate in excess of three (3) years of past performance and experience in the capacity and applications above will be awarded additional points during the selection process; one (1) point per year per application/program/data/interface/system for a maximum score of twenty-five (25) points. Offers which include experience in criminal justice programs including but not limited to TCIC, NCIC, CCH, TLETS and GJXDM/NIEM will receive an increase in score of one (1) point per year per type for a maximum of fifty (50) points.

## **5.11 Vendor Staff Experience**

Offers are required to demonstrate a minimum of three (3) years for each relevant staff member. The Vendor must provide information in their Offer response to indicate that the staff proposed has specific experience in providing the deliverables requested in this RFO. The following information is requested for staff assigned to this contract, including any subcontractors plus relevant application languages, hardware installation abilities, software upgrade experience, programming skills/abilities and data formats for each qualifying project. *Staff resumes must be identical in format and presentation.*

- Name
- Title
- Education
- Experience related to projects the staff member was directly involved in listed as the response to Section 5.9.2 and 5.10 (MUST include MM/YYYY)
  - Project(s) Scope
  - Role
  - Related specific technical qualification experience
  - Start and completion dates
- Specific work to be performed and/or deliverables to be provided under this contract

Offers received that sufficiently demonstrate in excess of three (3) years of past experience in the capacity and applications above will be awarded additional points during the selection process; one (1) point per year per application/program/data/interface/system for a maximum score of fifty (50) points.

### **5.12 Anti-Lobbying Affidavit (Appendix C)**

Vendor is required to execute an "Anti-Lobbying Affidavit," due at the time of the Offer submission. Affidavit form is provided (Appendix C). Execution of the affidavit indicates Vendor's agreement for purposes of this purchase that it shall not directly or indirectly communicate or attempt to communicate with TXDPS personnel, the evaluation committee members, or the other TXDPS officials involved in making recommendations or decisions for award of contract arising from this purchase, except through authorized, TXDPS sponsored communication mechanisms. Any such attempts of unauthorized communications after the posting of this RFO shall be deemed by TXDPS to be a Vendor's failure to comply with the terms and conditions of this purchase, and may result in rejection of the related Offer. For purposes of this subsection "directly or indirectly" includes employees, officials, agents and subcontractors of Vendor as well as unpaid associates, volunteers or other persons who would inquire, communicate or advocate consideration of a Vendor's Offer outside the selection process.

### **5.13 Affirmation Clauses and Preferences (Appendix D)**

Vendor must sign the attached "Affirmation Clauses," which are attached hereto and incorporated herein as Appendix "D." Failure of any Vendor to sign the attached "Affirmation Clauses" will result in rejection of Vendor's Offer.

### **5.14 HUB Subcontracting Plan (Appendix E)**

Historically Underutilized Business (HUB) Subcontracting Plan must be signed and accompany Vendor's Offer.

### **5.15 Non-Disclosure Agreement (Appendix F)**

Non-Disclosure Agreement (NDA) must be signed and submitted to obtain the CJIS Security Policy Packet Appendix G (described in Appendix F).

### **5.16 FBI CJIS Security Addendum (Appendix G)**

FBI CJIS Security Addendum (not attached, made available upon submission of an originally signed Non-Disclosure Agreement, Appendix F only). Vendor(s) evaluated by TXDPS as the best Offer(s) must execute an originally signed CJIS Security Addendum. Additionally, a CJIS Security Addendum Certification must be signed by each employee performing duties related to this project prior to final contract award. Each original Certification must include an original signature of the employee and a Vendor (Contractor) representative. Non-compliance by vendor will be cause for termination of contract negotiations and TXDPS may elect to enter into negotiations with the next highest evaluated Offer.

### **5.17 Contract (Appendix J)**

Vendor must not modify, revise or otherwise alter the Contract as posted. Any exceptions the Vendor may take to the Contract must be included in the Offer as a separate appendix and every exception must directly reference the specific Contract section and sub-section for each exception notated.

### **5.18 Service Level Agreement (Appendix K)**

Vendor must include all relevant Service Level Agreements (SLA), User Support Agreements, License Agreements, etc. with the Offer. Failure to include such documents or agreements defining the post-implementation responsibilities for the Vendor, TXDPS or local law enforcement may be cause for Offer disqualification.

### **5.19 Cost Offer**

Cost Offer in Appendix A must be signed and submitted separate from the Technical Offer. Vendor must ensure that the information provided in the Cost Offer is consistent with the information provided in the Technical Offer. The Cost Offer must be labeled, then bound and sealed separately from the Technical Offer. The Vendor is responsible for ensuring that the following identifying information appears on the outside of the package:

- “Sealed Cost Offer”
- “Project Name”
- “RFO ID: (Insert Number)”
- “Name and address of Vendor”

If a delivery service is used that prohibits such markings in the outside of the package, this information must be placed in plain view on the outside of an interior envelope or package.

## **6 ADDITIONAL REQUIREMENTS**

### **6.1 Prime Vendor and Subcontractors**

The Vendor responding to this posting must submit the Offer as a prime contractor with total accountability. While this does not preclude the use of subcontractors, the successful Vendor must assume single source responsibility and will be the sole point of contact for all system delivery, installation and operation, testing, training, warranty, maintenance, problem determination and resolution. If the Vendor expects to subcontract any part of the deliverables, the Vendor must clearly identify all subcontractors performing work on this project and their role and assignments for this Offer. All subcontractors' roles must be identified in the Vendor's Itemized Cost Breakdown. The Vendor must provide a statement from each subcontractor, signed by an individual authorized to legally obligate the subcontractor, attesting to the fact that the subcontractor has read the Offer and must provide the deliverables represented therein if Vendor is awarded the Contract. The Vendor must agree in its Offer to accept full responsibility for the performance of any subcontractor. All terms and conditions that apply to the Vendor apply to the subcontractor with the exception of single source responsibility. Each subcontractor may be required to submit ownership information as required by Vendor. The Vendor must disclose, at TXDPS' request, any information regarding subcontractors. Upon award of this contract, the prime awarded vendor will be required to provide copies of all subcontract agreements to TXDPS upon request.

## **6.2 Entities**

Each Offer shall be executed by only one entity, such as a corporation, a managing partner of a general or limited partnership, a joint venture, or other recognized legal entity. A prime contractor using subcontractors is an authorized arrangement.

The prime contractor must be identified in the Offer as well as subcontractors and their specific roles.

## **6.3 Public Information Act**

TXDPS is a governmental agency subject to the Texas Public Information Act. Offers submitted to TXDPS in response to the purchase are subject to release as public information after contract award. If the Vendor believes that the Offer, or parts of it, may be confidential, the Vendor must specify that either all or part of the Offer requires confidentiality and provide specific and detailed reasons for the exception to the rule. Vague and general claims to confidentiality are not acceptable. This is necessary so that TXDPS will have sufficient information to provide to the Office of the Attorney General (OAG) if an OAG opinion is requested. All Offers or parts of the Offers that are not marked as confidential automatically will be considered public information after a contract has been awarded. The successful Offer may be considered public information even though parts are marked "confidential." TXDPS will comply with the Public Information Act. TXDPS assumes no responsibility for asserting legal arguments on behalf of the Vendor. Vendor is advised to consult with their legal counsel concerning disclosure issues resulting from this Offer process and to take precautions to safeguard trade secrets and other proprietary information.

## **6.4 Contact Persons**

Vendor shall designate a person or persons whom TXDPS may contact to arrange and coordinate the creation and delivery of deliverables throughout the contract period.

## **6.5 Security**

Vendor must follow all TXDPS security policies. TXDPS will be given an opportunity to interview and investigate the person(s) proposed by the Vendor(s) prior to granting a security clearance. In addition, the FBI and TXDPS have computer security requirements (together with the CJIS Security Policy), including connections to the internet by any computer connected to TXDPS local area networks or mainframe system. The successful Vendor(s), including employees and sub-contractors working on this project, will be required to sign appropriate agreements and abide by these security requirements.

## **6.6 Electronic and Information Resources Accessibility Standards, As Required by 1 TAC Chapter 213 (Applicable to State Agency and Institution of Higher Education Purchases Only)**

1) Effective September 1, 2006 state agencies and institutions of higher education shall procure products which comply with the State of Texas Accessibility requirements for Electronic and Information Resources specified in 1 TAC Chapter 213 when such

products are available in the commercial marketplace or when such products are developed in response to a procurement solicitation.

2) Vendor shall provide TXDPS with the URL to its Voluntary Product Accessibility Template (VPAT) for reviewing compliance with the State of Texas Accessibility requirements (based on the federal standards established under Section 508 of the Rehabilitation Act), or indicate that the product/service accessibility information is available from the General Services Administration “Buy Accessible Wizard” (<http://www.buyaccessible.gov>). Vendors not listed with the “Buy Accessible Wizard” or supplying a URL to their VPAT must provide TXDPS with a report that addresses the same accessibility criteria in substantively the same format. Additional information regarding the “Buy Accessible Wizard” or obtaining a copy of the VPAT is located at <http://www.section508.gov/>

## **7 PURCHASING INFORMATION**

### **7.1 Offer Clarification**

TXDPS reserves the right to request Offer clarification on any product, technology, software, hardware, term or condition proposed. As part of the evaluation process, TXDPS may ask any or all Vendors to elaborate on or clarify specific portions of their Offers plus to continue to evaluate responses until such point as the best service and/or product is obtained for the State.

### **7.2 Contract Negotiation**

The TXDPS will establish a “Certified Provider” list and, at its own discretion, may populate the list with up to the top 4 (four) Vendors that meet the requirements of the RFO and whose responses are judged to qualify as a best service and product for the State. Participating local LEAs may select RRMS service from any of the Certified Providers on the list. TXDPS cannot guarantee that all Certified Providers on the list will be utilized by local LEAs and TXDPS makes no expressed or implied guarantees regarding minimum/maximum quantities or volumes.

Vendor are cautioned to propose their best possible Offers at the outset of the process as there is no guarantee that Best and Final Offers will be requested.

TXDPS reserves the right to negotiate any contract term or condition set forth by the Vendor that TXDPS considers to be unfavorable to the state or to local LEAs and to make modifications to the requirements set forth in this vendor specification document, provided such modifications do not constitute a substantial change. Negotiations shall be conducted until such time as TXDPS determines that the best service and product for the State has been obtained. All contract negotiations including any license, service level, user or technical support agreements, etc. must be initiated and completed prior to award.

### **7.3 Best Value Purchases**

TXDPS will use the best value factors in Section 2157.003 of the Texas Government Code as an evaluation component in making an award of any contract.

Texas Government Code, Title 10 2157.003 DETERMINING BEST VALUE FOR PURCHASES OF AUTOMATED INFORMATION SYSTEMS. "Best value" for purposes of this chapter means the lowest overall cost of an automated information system. In determining the lowest overall cost for a purchase or lease of an automated information system under this chapter, the commission or a state agency shall consider factors including:

- 7.3.1 the purchase price;
- 7.3.2 the compatibility to facilitate the exchange of existing data;
- 7.3.3 the capacity for expanding and upgrading to more advanced levels of technology;
- 7.3.4 quantitative reliability factors;
- 7.3.5 the level of training required to bring persons using the system to a stated level of proficiency;
- 7.3.6 the technical support requirements for the maintenance of data across a network platform and the management of the network's hardware and software;
- 7.3.7 the compliance with applicable Department of Information Resources statewide standards validated by criteria adopted by the department by rule; and
- 7.3.8 applicable factors listed in Sections 2155.074 and 2155.075.

Information obtained from the Texas Comptroller's Vendor Performance Tracking System may be used in evaluating Offers to solicitations for deliverables to determine the best value for the state.

#### **7.4 Offer Preparation Costs**

The State will not be responsible or liable for any costs incurred by any Vendor in the preparation and submission of its Offer or for other costs incurred by participating in this solicitation process.

#### **7.5 Piggy-Back Clause**

Certified Provider(s) agree to allow local Texas LEAs the option to participate in the Contract awarded as a result of this RFO under the same terms and conditions specified. Each Texas local LEA electing to utilize a Certified Provider under this Contract will issue a purchase order directly to the Certified Provider(s) referring to the terms and conditions specified in this RFO. Certified Provider(s) will invoice each agency directly. LEA may elect to implement the SLA executed under the TXDPS RRMS Contract OR the LEA may utilize the SLA executed under the TXDPS RRMS Contract plus negotiate SLA terms, conditions, services, performance, etc. providing they do not conflict with or weaken any term, condition, service, performance, etc. agreed upon through the executed TXDPS RRMS Contract, RRMS SLA, RRMS RFO, Vendor's original Offer including any appendices, addendum or amendments.

### **8 RMS SPECIFICATIONS**

This project is a deliverables-based turnkey solution in which the selected Vendor(s) will provide a secure environment for all aspects of the project deliverables for LEA Customers with limited or minimal technology resources. The RRMS Project is intended

to improve the effectiveness of the criminal justice community by providing the tools necessary to efficiently collect, evaluate, organize, analyze, and disseminate data associated with an incident cycle, including call for service reports, incident reports and arrest reports which occur in the jurisdiction(s) serviced by this project.

RMS Software includes records directly related to law enforcement operations such as incident, arrest, citation, warrant, case management, field contacts and other operational orientated records.

The proposed method of telecommunication or access must NOT require the *purchase* of any software, middleware, license, subscription, maintenance, support, etc. to use.

### **8.1 RMS Functionality**

Offers must list all standard elements, field length, and field content specifications (txt, char, txt/char, table driven, free text, etc). Offers must indicate the level of user customization (if available) associated with the data elements proposed for this section.

The following list of RMS functions must be fully described in the Vendor's Offer. RMS Software is not limited to the listed functions, nor are all the functions a mandatory requirement; however Offers will be evaluated based upon the all listed functions therefore Vendors are required to describe the RMS Software product capabilities for each function. Offers must include a complete listing of software elements which will be used during evaluation.

- 8.1.1** General System Requirements
- 8.1.2** Master Indices
- 8.1.3** Calls for Service
- 8.1.4** Incident Reporting
- 8.1.5** Investigative Case Management
- 8.1.6** Property and Evidence Management
- 8.1.7** Warrant
- 8.1.8** Arrest
- 8.1.9** Booking
- 8.1.10** Juvenile Contact
- 8.1.11** Crash Reporting
- 8.1.12** Citation
- 8.1.13** Field Contact
- 8.1.14** Pawn
- 8.1.15** Civil Process
- 8.1.16** Protection Orders and Restraints
- 8.1.17** Permits and Licenses
- 8.1.18** Equipment and Asset Management
- 8.1.19** Fleet Management
- 8.1.20** Personnel
- 8.1.21** Internal Affairs
- 8.1.22** Analytical Support

- 8.1.23 RMS Reports**
- 8.1.24 RMS System Administration**
- 8.1.25 RMS Interfaces**
- 8.1.26 Other**

## **8.2 N-DEx IEPD Elements**

The RMS Software must provide an adequate number of N-DEx based elements to capture data associated with a call for service report. The N-DEx IEPD does not specify minimum data sets for reporting calls for service, incidents nor arrest. Each vendor's Offer must enumerate the N-DEx based data elements that will be captured in the RMS Software. A portion of the scoring for the Offers will be based on the usefulness and the robustness of the data that the proposed RMS Software is able to accommodate (quantity and utility of elements). N-DEx IEPD specifications are located at: [NIEM N-DEx IEPD v. 2.0.0](#).

## **8.3 RMS Interfaces**

The RMS Software must be capable of interfacing/retrieving an existing record stored in a JMS Software product and/or a CAD Software product supplied by the same Vendor. Offers must describe interface capabilities with JMS and CAD Software as well as other standard interfaces or optional interfaces.

## **8.4 Livescan Interface**

The RMS Software must be capable of exporting arrest data in a form and content that is consistent with generating an EBTS compliant arrest transaction utilizing the Texas Type 2 record specification. Relevant specification documents are located at the following link: [EAR Packet](#).

## **8.5 Data Management**

### **8.5.1 Data Validation**

To ensure data integrity, the selected vendor(s) is requested to employ the data validation routines listed below.

### **8.5.2 Adult and Juvenile Subjects**

The RMS Software must be able to differentiate between records of a subject who is an adult (17 years of age [yoa] and above) from the records of a subject who is a juvenile (16 yoa and under). The RMS Software must differentiate the records based on the age of the subject at the time of the activity occurrence. Offers must describe methodology.

### **8.5.3 Duplicate Records**

The RMS Software must prohibit the creation of duplicate subject records within the system. Offers must describe methodology.

### **8.5.4 Global Data Standards**

The RMS Software must perform logical edit checks to ensure compliance with all applicable N-DEx standard values and formats prior to RMS Software data commitment or upon data export. Data must be compliant with NCIC and/or III data set edits. Offers

which perform logical edit checks prior to the commitment of data to the RMS Software will receive an increase in score. Offers must describe methodology.

### **8.5.5 Data Segregation**

The RMS Software must be able to logically separate the data belonging to one RMS Software agency user from the data of a different agency user. At no time should different agency's data be co-mingled within the RMS Software. Offers must describe methodology.

### **8.5.6 Arrest Data**

All data associated with an arrest must be validated according to standards established in the Texas Computerized Criminal History (CCH) Data Dictionary and the CCH Interface Document. Offers must describe methodology. Additionally, the RMS must be able to import identification responses from the livescan devices. Relevant specification documents are located at the following link: [EAR Packet](#).

### **8.6 Data Ownership**

Ownership of the data and/or images contained within the RMS Software will always remain with the contributing local LEA. Certified Providers may not copy, use nor disseminate the data in the RMS Software without express written consent of the contributing LEA.

### **8.7 Automated N-DEx NEIM IEPD**

Offers MUST include automated export functionality utilizing the N-DEx IEPD. Offers must describe functionality. N-DEx IEPD specifications are located at: [NIEM N-DEx IEPD v. 2.0.0](#).

### **8.8 Queries and Reports**

After a record query, the RMS Software must return all matching records for the selected criteria. The RMS Software must return specific information sought by the requestor. The RMS Software must have the ability to query and report large result sets.

#### **8.8.1 Record Locating Query**

The RMS Software must include, at a minimum, the ability to search for records by a combination of any or all of the following criteria:

**8.8.1.1** Name

**8.8.1.2** Alias or Nickname

**8.8.1.3** Identifying numbers, such as State ID number, State Issued Identification card number, Driver License number, Texas Youth Commission number, FBI number, Texas Department of Criminal Justice number, SSN, Case no., Miscellaneous number

#### **8.8.2 Predefined Queries**

The RMS Software must include, at a minimum, a standard set of predefined investigative, statistical and analytical reports to aid in the criminal investigative process.

### **8.8.3 Predefined Reports**

The RMS Software must include, at a minimum, a standard set of statistical and analytical reports to aid in the process of system administration. The following reports must be included in the predefined set of canned reports:

**8.8.3.1** List all users

**8.8.3.2** List all active users

**8.8.3.3** Log Report -- The Log Report will include information regarding user log in/log off, as well as, failures that occurred at log in, and any action taken by users against any records contained in RRMS.

### **8.8.4 Ad-Hoc Reports**

The RMS Software must provide system administrators with the capability to construct ad-hoc lists and statistical reports on all information contained within the RMS Software database.

## **8.9 Auditing**

The RMS Software must include an audit function, which will log all activity for a user agency within the database for all users from a specific LEA. Audit information must be able to identify transaction information including all transaction details, source credentials, and a time and date stamp of activity. This information must be available for review and analysis by system users based upon their user role in the system.

## **8.10 Security**

### **8.10.1 User Security and Authorization**

The user security and authorization must fully comply with the CJIS Security Policy (Appendix G). The RMS Software must facilitate security access utilizing unique user identifiers with role-based authorization.

The RMS Software must provide Advanced Authentication as required by the CJIS Security Policy. Vendors MUST completely describe the method for the proposed RMS Software Advanced Authentication including any costs or efforts which would be incurred by the Customers outside of RRMS Contract.

The RMS Software must include functionality that provides the local LEA user the ability to manage system users and roles in real-time. The RMS Software must provide the capability of creating and managing multiple access profiles. The local LEA user agency must be able to manage their own agency's user accounts and assign those accounts the various privileges established in the access profiles. The RMS Software must include functionality which allows authorized users to reset passwords upon request and profile/account verification.

The RMS Software must enforce password policies by restricting users from accessing the system after a finite number of failed attempts configurable by the Customer

administrator. Additionally, the system must automatically disable user accounts after a set period of non-use configured by the Customer administrator.

Following a set amount of time of inactivity during the LEA User's session, the RMS Software must automatically end a user session. The inactivity time period must be configurable by the customer administrator.

Vendor *must* describe the RMS Software User Security and Authentication methodology including:

- 8.10.1.1 level, type, hierarchy and quantity of role based profiles functionality, configurable events, etc.
- 8.10.1.2 User data or information necessary to create/maintain account
- 8.10.1.3 Minimum and maximum number of failed attempts, and
- 8.10.1.4 Minimum and maximum time periods of inactivity allowed for:
  - 8.10.1.4.1 During any single session
  - 8.10.1.4.2 Between sessions
  - 8.10.1.4.3 Other

### **8.10.2 System Security**

TXDPS requires that Offers demonstrate an understanding of the CJIS Security Policy and its requirements (Appendix G). The host and remote RMS Software must fully comply with the requirements contained in the CJIS Security Policy. Vendors are required to sign and submit Affirmation Clauses (Appendix D) as acknowledgment they have read and understand the security requirements articulated in the FBI's CJIS Security policy and, if selected as a certified provider, will execute a CJIS Security Addendum in conjunction with the associated RRMS Contract.

### **8.11 Expandability**

The RMS Software must be designed and configured to allow for future expansion, in order to accommodate the addition of new stakeholders, as they become ready to participate.

### **8.12 Training and Documentation**

#### **8.12.1 Training**

TXDPS will require the successful Vendor(s) to provide training for TXDPS and local LEAs technical and administrative staff members. Offers must supply a training plan that addresses training for the following:

- 8.12.1.1 End User
- 8.12.1.2 System Administrator
- 8.12.1.3 Configuration Staff
- 8.12.1.4 Support Staff

Training must occur between twenty-one (21) and seven (7) days prior to an agency going live with a selected Certified Provider. The selected Certified Provider must

provide updated training concerning maintenance code releases to the RRMS LEA Users and TXDPS staff prior to code release implementation. TXDPS must approve all training materials, media or forums prior to utilization. Offers must contain a training plan which includes at a minimum:

- 8.12.1.5** Description of the training event
- 8.12.1.6** Description of the methods of delivery that will be used (hands-on, computer based training, online, combination, etc)
- 8.12.1.7** Specifics regarding communication procedures, protocols, etc to facilitate training attendance for all stakeholders
- 8.12.1.8** Maximum and minimum class size
- 8.12.1.9** Quantity of training events
- 8.12.1.10** Methods for evaluation and feedback and how that feedback will be used; and
- 8.12.1.11** Length of training event

### **8.12.2 Documentation**

Documentation pertinent to the RMS Software System must be provided or made available on demand to TXDPS and the local agency user. Documentation must be understandable and is subject to review prior to acceptance. Certified Providers must update all relevant documentation regarding the affected system and must have PM approval prior to implementing all maintenance releases. Required documentation includes, but is not limited to:

- 8.12.2.1** System Architecture Document and Diagram
- 8.12.2.2** System Administrator Documentation
- 8.12.2.3** End User Documentation including FAQ's and responses
- 8.12.2.4** Agency Interface documentation

Documentation must be provided or made available on demand to TXDPS and local agency users no later than three (3) weeks before the first agency selecting that Certified Provider goes live. Offers which provide electronic documentation available through the RMS Software will receive an increase in score. The RMS Software Offer must provide a comprehensive strategy to communicate with stakeholders. TXDPS must approve all documentation materials prior to utilization. The Offer must include at a minimum:

- 8.12.2.5** Description and sample of the types of documentation
- 8.12.2.6** Description of the methods of delivery that will be used
- 8.12.2.7** Specifics regarding communication procedures, protocols, etc. to facilitate documentation dissemination for all stakeholders; and
- 8.12.2.8** Release schedule

### **8.13 LEA Responsibilities**

Offers must list the responsibilities imposed upon the LEA as a user and/or a host site concerning;

- software (OS, RMS, middleware, etc)

- installation
- maintenance
- updates
- hardware
  - installation
  - maintenance
  - upgrades
- training
- vendor site access, site preparation or site requirements
- project management
  - scheduling
  - testing
  - implementation
  - change control
- data management
- data migration
- user management
- telecommunications
- Other (list any other responsibilities not specifically identified above)

## **9 JMS SPECIFICATIONS**

A Jail Management System (JMS) will have the ability to record the initial processing of offenders and maintain data related to their activities and tracking during the period of their incarceration.

The proposed method of telecommunication or access must NOT require the *purchase* of any software, middleware, license, subscription, maintenance, support, etc. to use.

### **9.1 JMS Functionality**

Offers must list all standard elements, field length, and field content specifications (txt, char, txt/char, table driven, free text, etc). Offers must indicate the level of user customization (if available) associated with the data elements proposed for this section.

The following list of JMS functions must be fully described in the Vendor's Offer. JMS Software is not limited to the listed functions nor are all functions a mandatory requirement; however, Vendors are required to describe the JMS Software product capabilities for each function. Offers must include a complete listing of software elements which will be used during evaluation.

#### **9.1.1 General System Requirements**

#### **9.1.2 Offender Admission**

#### **9.1.3 Offender Management**

#### **9.1.4 Offender Disciplinary Process**

#### **9.1.5 Administrative Functions**

##### **9.1.5.1 Shift Report**

##### **9.1.5.2 Personnel**

- 9.1.5.3 Facility Statistics
- 9.1.6 Offender Health Care
  - 9.1.6.1 Offender Disposition
  - 9.1.6.2 Release and Discharge
- 9.1.7 Community Supervision
- 9.1.8 Property and Evidence Management
- 9.1.9 DNA Collection status
- 9.1.10 Equipment and Asset Management
- 9.1.11 Fleet Management
- 9.1.12 JMS Reports
- 9.1.13 JMS System Administration
- 9.1.14 JMS Interfaces
- 9.1.15 Other

## **9.2 N-DEx IEPD Elements**

The JMS Software must provide an adequate number of N-DEx based elements to capture data associated with a call for service report. The N-DEx IEPD does not specify minimum data sets for reporting calls for service, incidents nor arrest. Each vendor's Offer must enumerate the N-DEx based data elements that will be captured in the JMS Software. A portion of the scoring for the Offers will be based on the usefulness and the robustness of the data that the proposed JMS Software is able to accommodate (quantity and utility of elements). N-DEx IEPD specifications are located at: [NIEM N-DEx IEPD v. 2.0.0](#).

## **9.3 JMS Interfaces**

The JMS Software must be capable of interfacing/retrieving an existing record stored in a RMS Software product and/or a CAD Software product supplied by the same Vendor. Offers must describe interface capabilities with RMS and CAD Software as well as other standard interfaces or optional interfaces.

### **9.3.1 Livescan Interface**

The JMS Software must be capable of exporting arrest data in a form and content that is consistent with generating an EBTS compliant arrest transaction utilizing the Texas Type 2 record specification. Additionally, the JMS must be able to import identification responses from the livescan devices. Relevant specification documents are located at the following link: [EAR Packet](#).

## **9.4 Data Management**

### **9.4.1 Data Validation**

To ensure data integrity, the selected vendor(s) is requested to employ the data validation routines listed below.

### **9.4.2 Adult and Juvenile Subjects**

JMS must be able to differentiate between records of a subject who is an adult (17 yoa and above) from the records of a subject who is a juvenile (16 yoa and under). JMS

must differentiate the records based on the age of the subject at the time of the activity occurrence. Offers must describe methodology.

#### **9.4.3 Duplicate Records**

JMS must prohibit the creation of duplicate subject records within the system. Offers must describe methodology.

#### **9.4.4 Global Data Standards**

JMS must perform logical edit checks to ensure compliance with all applicable N-DEx standard values and formats prior to JMS data commitment or upon data export. Data must be compliant with NCIC and/or III data set edits. Offers which perform logical edit checks prior to the commitment of data to the JMS will receive an increase in score. Offers must describe methodology.

#### **9.4.5 Data Segregation**

JMS must be able to logically separate the data belonging to one JMS agency user from the data of a different agency user. At no time should different agency's data be co-mingled within the JMS. Offers must describe methodology.

#### **9.4.6 Arrest Data**

All data associated with an arrest must be validated according to standards established in the Texas Computerized Criminal History (CCH) data dictionary and the CCH Interface Document. Offers must describe methodology. Additionally, the JMS must be able to import identification responses from the livescan devices. Relevant specification documents are located at the following link: [EAR Packet](#).

#### **9.5 Data Ownership**

Ownership of the data and/or images contained within the JMS will always remain with the contributing local LEA. Certified Providers may not copy, use nor disseminate the data in the JMS without express written consent of the contributing LEA.

#### **9.6 Automated N-DEx NEIM IEPD**

Offers MUST include automated export functionality utilizing the N-DEx IEPD. Offers must describe functionality. N-DEx IEPD specifications are located at: [NIEM N-DEx IEPD v. 2.0.0](#).

#### **9.7 Queries and Reports**

After a record query, JMS must return all matching records for the selected criteria. RRMS must return specific information sought by the requestor. JMS must have the ability to query and report large result sets.

##### **9.7.1 Record Locating Query**

JMS must include, at a minimum, the ability to search for records by a combination of any or all of the following criteria:

###### **9.7.1.1 Name**

**9.7.1.2** Alias or Nickname

**9.7.1.3** Identifying numbers, such as State ID number, State Issued Identification card number, Driver License number, Texas Youth Commission number, FBI number, Texas Department of Criminal Justice number, SSN, Case no., Miscellaneous number

### **9.7.2 Predefined Queries**

JMS must include, at a minimum, a standard set of predefined investigative, statistical and analytical reports to aid in the criminal investigative process.

### **9.7.3 Predefined Reports**

JMS must include, at a minimum, a standard set of statistical and analytical reports to aid in the process of system administration. The following reports must be included in the predefined set of canned reports:

**9.7.3.1** List all users

**9.7.3.2** List all active users

**9.7.3.3** Log Report -- The Log Report will include information regarding user log in/log off, as well as, failures that occurred at log in, and any action taken by users against any records contained in RRMS

### **9.7.4 Ad-Hoc Reports**

JMS must provide system administrators with the capability to construct ad-hoc lists and statistical reports on all information contained within the JMS database.

## **9.8 Auditing**

The JMS Software must include an audit function, which will log all activity for a user agency within the database for all users from a specific LEA. Audit information must be able to identify transaction information including all transaction details, source credentials, and a time and date stamp of activity. This information must be available for review and analysis by system users based upon their user role in the system.

## **9.9 Security**

### **9.9.1 User Security and Authorization**

The user security and authorization must fully comply with the CJIS Security Policy (Appendix G). The JMS Software must facilitate security access utilizing unique user identifiers with role-based authorization.

The JMS Software must provide Advanced Authentication as required by the CJIS Security Policy. Vendors MUST completely describe the method for the proposed JMS Software Advanced Authentication including any costs or efforts which would be incurred by the Customers outside of RRMS Contract.

The JMS Software must include functionality that provides the local LEA user the ability to manage system users and roles in real-time. The JMS Software must provide the capability of creating and managing multiple access profiles. The local LEA user

agency must be able to manage their own agency's user accounts and assign those accounts the various privileges established in the access profiles. The JMS Software must include functionality which allows authorized users to reset passwords upon request and profile/account verification.

The JMS Software must enforce password policies by restricting users from accessing the system after a finite number of failed attempts configurable by the Customer administrator. Additionally, the system must automatically disable user accounts after a set period of non-use configured by the Customer administrator.

Following a set amount of time of inactivity during the LEA User's session, the JMS Software must automatically end a user session. The inactivity time period must be configurable by the customer administrator.

### **9.9.2 System Security**

TXDPS requires that Offers demonstrate an understanding of the CJIS Security Policy and its requirements (Appendix G). The host and remote JMS Software must fully comply with the requirements contained in the CJIS Security Policy. Vendors are required to sign and submit Affirmation Clauses (Appendix D) as acknowledgment they have read and understand the security requirements articulated in the FBI's CJIS Security policy and, if selected as a certified provider, will execute a CJIS Security Addendum in conjunction with the associated RRMS Contract.

### **9.10 Expandability**

The JMS Software must be designed and configured to allow for future expansion, in order to, accommodate the addition of new stakeholders, as they become ready to participate.

### **9.11 Training and Documentation**

#### **9.11.1 Training**

TXDPS will require the successful Vendor(s) to provide training for TXDPS and local LEAs technical and administrative staff members. Offers must supply a training plan that addresses training for the following:

**9.11.1.1** End User

**9.11.1.2** System Administrator

**9.11.1.3** Configuration Staff

**9.11.1.4** Support Staff

Training must occur between twenty-one (21) and seven (7) days prior to an agency going live with a selected Certified Provider. The selected Certified Provider must provide updated training concerning maintenance code releases to the RRMS LEA Users and TXDPS staff prior to code release implementation. TXDPS must approve all training materials, media or forums prior to utilization. Offers must contain a training plan which includes at a minimum:

- 9.11.1.5 Description of the training event
- 9.11.1.6 Description of the methods of delivery that will be used (hands-on, computer based training, online, combination, etc)
- 9.11.1.7 Specifics regarding communication procedures, protocols, etc to facilitate training attendance for all stakeholders
- 9.11.1.8 Maximum and minimum class size
- 9.11.1.9 Quantity of training events
- 9.11.1.10 Methods for evaluation and feedback and how that feedback will be used; and
- 9.11.1.11 Length of training event

### **9.11.2 Documentation**

Documentation pertinent to the JMS Software System must be provided or made available on demand to TXDPS and the local agency user. Documentation must be understandable and is subject to review prior to acceptance. Certified Providers must update all relevant documentation regarding the affected system and must have PM approval prior to implementing all maintenance releases. Required documentation includes, but is not limited to:

- 9.11.2.1 System Architecture Document and Diagram
- 9.11.2.2 System Administrator Documentation
- 9.11.2.3 End User Documentation including FAQ's and responses
- 9.11.2.4 Agency Interface documentation

Documentation must be provided or made available on demand to TXDPS and local agency users no later than three (3) weeks before the first agency selecting that Certified Provider goes live. The JMS Software Offer must provide a comprehensive strategy to communicate with stakeholders. TXDPS must approve all documentation materials prior to utilization. The Offer must include at a minimum:

- 9.11.2.5 Description and sample of the types of documentation;
- 9.11.2.6 Description of the methods of delivery that will be used;
- 9.11.2.7 Specifics regarding communication procedures, protocols, etc to facilitate documentation dissemination for all stakeholders; and
- 9.11.2.8 Release schedule.

### **9.12 LEA Responsibilities**

Offers must list the responsibilities imposed upon the LEA as a user and/or a host site concerning;

- software (OS, JMS, middleware, etc),
  - installation
  - maintenance
  - updates
- hardware,
  - installation
  - maintenance
  - upgrades

- training,
- vendor site access, site preparation or site requirements,
- project management
  - scheduling
  - testing
  - implementation
  - change control
- data management,
- data migration,
- user management,
- telecommunications,
- Other (list any other responsibilities not specifically identified above).

## **10 CAD SPECIFICATIONS**

CAD involves those functions primarily performed during a call for service or dispatch services including type of service, location and time, circumstances, relevant identifiers, etc.

The proposed method of telecommunication or access must NOT require the *purchase* of any software, middleware, license, subscription, maintenance, support, etc. to use.

### **10.1 CAD Functionality**

Offers must list all standard elements, field length, and field content specifications (txt, char, txt/char, table driven, free text, etc). Offers must indicate the level of user customization (if available) associated with the data elements proposed for this section.

The following list of CAD functions must be fully described in the Vendor's Offer. CAD Software is not limited to the listed functions nor are all functions a mandatory requirement; however, Vendors are required to describe the CAD Software product capabilities for each function. Offers must include a complete listing of software elements which will be used during evaluation.

- 10.1.1** Law Enforcement Dispatch
- 10.1.2** CAD System Administrators
- 10.1.3** Support Services
- 10.1.4** Traffic Stops/Abandon Vehicles
- 10.1.5** Call Management and Management Reporting
- 10.1.6** Interfaces
- 10.1.7** EMS Dispatch
- 10.1.8** Fire Dispatch
- 10.1.9** Warrants
- 10.1.10** Wrecker Rotation
- 10.1.11** Intelligent Transportation
- 10.1.12** Properties
- 10.1.13** Other

CAD proposals should incorporate the Law Enforcement Information Technology Standards Council (LEITSC) Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (Appendix L).

## **10.2 CAD Interfaces**

The CAD Software must be capable of interfacing/retrieving an existing record stored in a RMS Software product and/or a JMS Software product supplied by the same Vendor. Offers must describe interface capabilities with RMS and JMS Software as well as other standard interfaces or optional interfaces.

## **10.3 Data Management**

### **10.3.1 Data Validation**

To ensure data integrity, the selected vendor(s) is requested to employ the data validation routines listed below.

### **10.3.2 Global Data Standards**

CAD must perform logical edit checks to ensure compliance with all applicable N-DEX standard values and formats prior to CAD data commitment or upon data export. Data must be compliant with NCIC and/or III data set edits as applicable. Offers which perform logical edit checks prior to the commitment of data to the CAD will receive an increase in score. Offers must describe methodology.

### **10.3.3 Data Segregation**

CAD must be able to logically separate the data belonging to one CAD agency user from the data of a different agency user. At no time should different agency's data be co-mingled within the CAD. Offers must describe methodology.

## **10.4 Data Ownership**

Ownership of the data and/or images contained within the CAD will always remain with the contributing local LEA. Certified Providers may not copy, use nor disseminate the data in the CAD without express written consent of the contributing LEA.

## **10.5 Automated N-DEX NEIM IEPD**

Offers MUST include automated export functionality utilizing the N-DEX IEPD. Offers must describe functionality. N-DEX IEPD specifications are located at: [NIEM N-DEX IEPD v. 2.0.0](#).

## **10.6 Queries and Reports**

After a record query, CAD must return all matching records for the selected criteria. CAD must return specific information sought by the requestor. CAD must have the ability to query and report large result sets.

### **10.6.1 Predefined Queries**

CAD must include, at a minimum, a standard set of predefined investigative, statistical and analytical reports to aid in the criminal investigative process.

### **10.6.2 Predefined Reports**

CAD must include, at a minimum, a standard set of statistical and analytical reports to aid in the process of system administration. The following reports must be included in the predefined set of canned reports:

**10.6.2.1** List all users

**10.6.2.2** List all active users

**10.6.2.3** Log Report -- The Log Report will include information regarding user log in/log off, as well as, failures that occurred at log in, and any action taken by users against any records contained in RRMS

### **10.6.3 Ad-Hoc Reports**

CAD must provide system administrators with the capability to construct ad-hoc lists and statistical reports on all information contained within the CAD database.

## **10.7 Auditing**

The CAD Software must include an audit function, which will log all activity for a user agency within the database for all users from a specific LEA. Audit information must be able to identify transaction information including all transaction details, source credentials, and a time and date stamp of activity. This information must be available for review and analysis by system users based upon their user role in the system.

## **10.8 Security**

### **10.8.1 User Security and Authorization**

The user security and authorization must fully comply with the CJIS Security Policy (Appendix G). The CAD Software must facilitate security access utilizing unique user identifiers with role-based authorization.

The CAD Software must provide Advanced Authentication as required by the CJIS Security Policy. Vendors MUST completely describe the method for the proposed CAD Software Advanced Authentication including any costs or efforts which would be incurred by the Customers outside of RRMS Contract.

The CAD Software must include functionality that provides the local LEA user the ability to manage system users and roles in real-time. The CAD Software must provide the capability of creating and managing multiple access profiles. The local LEA user agency must be able to manage their own agency's user accounts and assign those accounts the various privileges established in the access profiles. The RMS Software must include functionality which allows authorized users to reset passwords upon request and profile/account verification.

The CAD Software must enforce password policies by restricting users from accessing the system after a finite number of failed attempts configurable by the Customer administrator. Additionally, the system must automatically disable user accounts after a set period of non-use configured by the Customer administrator.

Following a set amount of time of inactivity during the LEA User's session, the CAD Software must automatically end a user session. The inactivity time period must be configurable by the customer administrator.

### **10.8.2 System Security**

TXDPS requires that Offers demonstrate an understanding of the CJIS Security Policy and its requirements (Appendix G). The host and remote CAD Software must fully comply with the requirements contained in the CJIS Security Policy. Vendors are required to sign and submit Affirmation Clauses (Appendix D) as acknowledgment they have read and understand the security requirements articulated in the FBI's CJIS Security policy and, if selected as a certified provider, will execute a CJIS Security Addendum in conjunction with the associated RRMS Contract.

### **10.9 Expandability**

The CAD Software must be designed and configured to allow for future expansion, in order to accommodate the addition of new stakeholders, as they become ready to participate.

### **10.10 Training and Documentation**

#### **10.10.1 Training**

TXDPS will require the successful Vendor(s) to provide training for TXDPS and local LEAs technical and administrative staff members. Offers must supply a training plan with their response which addresses training for the following:

##### **10.10.1.1 End User**

##### **10.10.1.2 System Administrator**

##### **10.10.1.3 Configuration Staff**

##### **10.10.1.4 Support Staff**

Training must occur between twenty-one (21) and seven (7) days prior to an agency going live with a selected Certified Provider. The selected Certified Provider must provide updated training concerning maintenance code releases to the RRMS LEA Users and TXDPS staff prior to code release implementation. TXDPS must approve all training materials, media or forums prior to utilization. Offers must contain a training plan which includes at a minimum:

##### **10.10.1.5 Description of the training event**

##### **10.10.1.6 Description of the methods of delivery that will be used (hands-on, computer based training, online, combination, etc)**

##### **10.10.1.7 Specifics regarding communication procedures, protocols, etc to facilitate training attendance for all stakeholders**

**10.10.1.8** Maximum and minimum class size

**10.10.1.9** Quantity of training events

**10.10.1.10** Methods for evaluation and feedback and how that feedback will be used;  
and

**10.10.1.11** Length of training event

## **10.10.2 Documentation**

Documentation pertinent to the CAD Software System must be provided or made available on demand to TXDPS and the local agency user. Documentation must be understandable and is subject to review prior to acceptance. Certified Providers must update all relevant documentation regarding the effected system and must have PM approval prior to implementing all maintenance releases. Required documentation includes, but is not limited to:

**10.10.2.1** System Architecture Document and Diagram

**10.10.2.2** System Administrator Documentation

**10.10.2.3** End User Documentation including FAQ's and responses

**10.10.2.4** Agency Interface documentation

Documentation must be provided or made available on demand to TXDPS and local agency users no later than three (3) weeks before the first agency selecting that Certified Provider goes live. The CAD Software Offer must provide a comprehensive strategy to communicate with stakeholders. TXDPS must approve all documentation materials prior to utilization. The Offer must include at a minimum:

**10.10.2.5** Description and sample of the types of documentation

**10.10.2.6** Description of the methods of delivery that will be used

**10.10.2.7** Specifics regarding communication procedures, protocols, etc to facilitate documentation dissemination for all stakeholders; and

**10.10.2.8** Release schedule

## **10.11 LEA Responsibilities**

Offers must list the responsibilities imposed upon the LEA as a user and/or a host site concerning;

- software (OS, CAD, middleware, etc)
  - installation
  - maintenance
  - updates
- hardware
  - installation
  - maintenance
  - upgrades
- training
- vendor site access, site preparation or site requirements
- project management
  - scheduling

- testing
- implementation
- change control
- data management
- data migration
- user management
- telecommunications
- Other (list any other responsibilities not specifically identified above)

## **11 Software and Hardware**

### **11.1 Software**

Offers must supply a list of any software products not included in the Offer that local LEA users will need in order to use the selected RRMS system. The software list must include the software name as well as the version and/or release. The proposed RMS Software, JMS Software and/or CAD Software must NOT require the *purchase* of any additional software, middleware, license, subscription, maintenance, support, etc. to use.

### **11.2 Hardware**

Offers must provide the minimum hardware specifications necessary for stakeholders to access the RRMS such as Operating System, web application, etc. Offers must provide the minimum hardware specifications necessary for stakeholders to host the RRMS should the LEA prefer to utilize existing hardware or independently purchase and own hosting hardware.

### **11.3 Hosting**

Offers must describe the hosting plan which will be utilized for the Certified Provider hosted RRMS. All hardware, software application and data will be housed at the Certified Provider's CJIS approved facilities, the local law enforcement agency or TXDPS. Offers must describe their hosting strategy and any cost saving initiatives including but not limited to the following items:

#### **11.3.1 Hardware, software, applications and platforms**

##### **11.3.1.1 Certified Provider**

##### **11.3.1.2 Local law enforcement agency**

##### **11.3.1.3 TXDPS**

#### **11.3.2 System administration (including enhancements, maintenance and support)**

##### **11.3.2.1 Certified Provider**

##### **11.3.2.2 Local law enforcement agency**

##### **11.3.2.3 TXDPS**

#### **11.3.3 Server and infrastructure administration (including upgrades, maintenance and support)**

##### **11.3.3.1 Certified Provider**

##### **11.3.3.2 Local law enforcement agency**

##### **11.3.3.3 TXDPS**

#### **11.3.4 Hosting/facility location**

- 11.3.4.1 Certified Provider
- 11.3.4.2 Local law enforcement agency
- 11.3.4.3 TXDPS
- 11.3.5 System operation monitoring
  - 11.3.5.1 Certified Provider
  - 11.3.5.2 Local law enforcement agency
  - 11.3.5.3 TXDPS
- 11.3.6 Production control and scheduling
  - 11.3.6.1 Certified Provider
  - 11.3.6.2 Local law enforcement agency
  - 11.3.6.3 TXDPS
- 11.3.7 Storage management
  - 11.3.7.1 Certified Provider
  - 11.3.7.2 Local law enforcement agency
  - 11.3.7.3 TXDPS
- 11.3.8 Backups and disaster recovery plan
  - 11.3.8.1 Certified Provider
  - 11.3.8.2 Local law enforcement agency
  - 11.3.8.3 TXDPS
- 11.3.9 Security controls (physical and logical)
  - 11.3.9.1 Certified Provider
  - 11.3.9.2 Local law enforcement agency
  - 11.3.9.3 TXDPS
- 11.4 Customer reports for system status– frequency and types
  - 11.4.1.1 Certified Provider
  - 11.4.1.2 Local law enforcement agency
  - 11.4.1.3 TXDPS
- 11.4.2 Data quantity or size scale
  - 11.4.2.1 Certified Provider
  - 11.4.2.2 Local law enforcement agency
  - 11.4.2.3 TXDPS

Vendors are not prohibited from contracting with local LEAs to host the RRMS providing both the hosting local LEAs as well as the customer local LEAs are mutually agreeable to the arrangement.

## **12 SYSTEM FUNCTIONALITY**

### **12.1 Project Deliverable Schedule**

Time is of the essence. Offers supplying a more aggressive timeline will receive additional points in the scoring process. The Offer must provide a project deliverable schedule that identifies major milestones including but not limited to program specification gathering, development, testing, installation, and data conversion services in the vendor response to this RFO. Time is of the essence, Offer with the most aggressive deliverable schedule to reach 100% Final Operating Capability (FOC defined in Section 12.2) and evaluated by TXDPS as realistically achievable.

## **12.2 Final Operating Capability**

Final operating capability (FOC) is defined as complete implementation with successful LEA testing and final local user agency approval including 10 days of error free application utilization by the local user agency prior to approval. The FOC procedure must be repeated for each installation of RRMS at a local LEA. Vendor's PM will be required to provide to the TXDPS PM or LEA PM a FOC document to collect original signatures from the vendor, LEA and TXDPS which mutually agrees to full acceptance of a specific RRMS local implementation. Vendor may not submit an invoice for an RRMS site until the FOC document has been approved by original signatures by all parties.

## **12.3 Warranty**

All deliverables of the RRMS System Project are subject to Vendor warranty. Vendor must warranty all deliverables for a minimum of a 12 month period immediately following fully approved FOC.

## **12.4 Data Backup and Disaster Recovery**

Offers must include the Vendor's strategy for data backup, storage management (disk, tape), and disaster recovery/backups. Offers which offer offsite storage of backups may receive an increase in score.

## **13 SOFTWARE LICENSES**

The RRMS Software License MUST NOT impose overly restrictive administrative management practices or limitations regarding:

- 13.1** Type of User accounts
- 13.2** Quantities of searches or queries conducted
- 13.3** Quantity, volume or size of record contributions and/or storage
- 13.4** Quantity of workstation installations (if applicable)

Customer License should be based upon the total number of active User accounts and Offers should use the scalable factors identified in Section 2.3 Stakeholders for the basis of the annual license cost.

## **14 RRMS MODIFICATIONS OR ENHANCEMENTS**

Future modifications or enhancements (post-implementation) in the original scope of the RRMS Contract may be necessary to accommodate new or increased functionality required by legislation, criminal justice initiatives, LEAs request, etc. Modifications or enhancements will be accomplished through a Statement of Work (SOW). The following elements are the minimum requirements for all SOW's issued:

- 14.1** Complete project scope and definition
- 14.2** Type of work (application development, web development, etc.)
- 14.3** Quantity of hours per type of work
- 14.4** Cost per type of work
- 14.5** Schedule

- 14.6 Responsibilities of all Parties involved
- 14.7 Project dependencies
- 14.8 Acceptance criteria
- 14.9 Vendor PM (name, address and phone numbers)
- 14.10 Customer PM (name, address and phone numbers)
- 14.11 Project Completion Acceptance Form

SOWs must be signed and dated by TXDPS PM or LEA PM and Vendor prior to beginning of any work. The SOW project completion acceptance page must collect signature and date of TXDPS PM or LEA PM and the Vendor following the conclusion of the modifications or enhancements to verify acceptable project completion by all Parties. Vendor may submit invoice(s) following signatures by all Parties on the Acceptance Form.

**15 EVALUATION CRITERIA**

Only those Offers that are deemed to be in administrative compliance will be evaluated for responsiveness to the state's needs. State agencies are responsible for determining "Best Value" when making procurement decisions related to Automated Information Systems (AIS)/Telecommunications component or services. A state agency may purchase or lease Automated Information Systems (AIS)/Telecommunications component or services directly from a vendor and may negotiate additional terms and conditions to be included in contracts relating to the purchase or lease. This is provided if the purchase or lease is based on the best value available and is in the state's best interest. In determining which products or services are in the state's best interest, the agency shall consider Section 2157.003 of the Texas Government Code.

<b>RFO Response Component</b>	<b>Maximum Points Assessed</b>	<b>Maximum Percentage</b>
Overall Offer Cost Per Agency (Appendix A)	402.50	40%
Qualifications and References of Vendor (Sections 5.9)	50.00	5%
Additional Vendor Qualifications (Section 5.10)	50.00	5%
Vendor Staff Experience (Section 5.11)	50.00	5%
Service Level Agreement (Section 5.19/Appendix K)	50.00	5%
RMS Specifications (Section 8)	227.50	23%
Hardware and Software (Section 11)	50.00	5%
System Functionality (Section 12)	60.00	6%
Software Licenses (Section 13)	60.00	6%
<b>TOTAL</b>	<b>1,000.00</b>	<b>100%</b>

**16 ATTACHED CONTRACT**

As part of the award process, the successful Vendor(s) must sign the attached contract, which is attached hereto and incorporated herein as Appendix J; TXDPS hereby

expressly rejects any exceptions to or additions to the attached contract that Vendor submits with its Offer. Any exceptions to or additions to the attached contract will only become part of the final contract if TXDPS expressly agrees to such exceptions or additions. Vendor must fill the blanks in Section I. Parties, Section 38. Notices, as well as signatory page.

If Vendor has any objection to any language in the attached contract, Vendor must provide the language (including the section number) to which Vendor has an objection, state the basis for the objection and propose substitute language.

TXDPS reserves the right to make changes to the attached contract prior to execution of the attached contract.

## **17 CONTRACT TERM**

Each Vendor selected as a Certified Provider will be required to sign the Contract prior to being placed on the Certified RRMS Provider List. Each contract shall become effective on the date it is signed by the last of the two parties to an instance of this Contract. The initial term of this Contract shall last for two (2) years after execution of this contract by the initial Certified Provider.

TXDPS reserves the right to renew this Agreement with any Certified Provider(s), in whole or in part under the same terms and conditions, for up to six (6) years in increments of up to two (2) years each. In no case shall the full term of the Contract including extensions exceed eight (8) years. TXDPS will exercise this option by providing written notice to the Certified Provider prior to the expiration of this Agreement. Any renewal will only become effective after both Parties sign a document to renew this Agreement.

In addition to the rights granted to TXDPS above, TXDPS also has the right, at its own election, to extend the Contract for ninety (90) days beyond the expiration of any initial or renewal term. TXDPS will exercise this unilateral right by providing notice to the Certified Provider before the end of any initial or renewal term of the Contract.

## **18 APPENDICES**

Appendices A – L. Appendices A through L are part of this RFO for all purposes. All appendices are included within this RFO, are attached as Offer packages, or will be made available upon request by vendor submission of an originally signed Non-Disclosure Agreement (Appendix F) and made a part of this requisition. Appendices not posted but available through submission of Appendix G are available by electronic means (e-mail, CD, or floppy), facsimile, hardcopy by mail, or hard copy by vendor personal courier. It is the responsibility of the vendor to notify the TXDPS purchaser of vendor's preference for the method of receiving appendices that are not posted with this RFO.

- Appendix A: Cost Offer
- Appendix B: Vendor Information **(Must sign and submit with Offer)**

- Appendix C: Anti-Lobbying Affidavit **(Must sign and submit with Offer)**
- Appendix D: Affirmation Clauses **(Must sign and submit with Offer)**
- Appendix E: HUB Subcontracting Plan **(Must sign and submit with Offer)**
- Appendix F: Non-Disclosure Agreement **(Must be submitted to obtain Appendix G,)**
- Appendix G: FBI CJIS Security Policy Packet **(Required prior to Contract execution)**
- Appendix H: Dissemination of Criminal History Record Information
- Appendix I: Title 28, Code of Federal Regulations, Part 20
- Appendix J: Contract
- Appendix K: Service Level Agreement/User Support
- Appendix L: Law Enforcement Information Technology Standards Council (LEITSC) Standard Functional Specifications for Law Enforcement Computer Aided Dispatch

## APPENDIX A

### TXDPS RRMS RFO COST OFFER

**The Cost Offer must be signed, labeled, then bound and sealed separately from the Technical Offer. Any Offers that do not clearly and accurately itemize each cost could be cause for rejection.**

Vendor must ensure that the information provided in the Cost Offer is consistent with the information provided in the Technical Offer. The Cost Offer must be labeled, then bound and sealed separately from the Technical Offer. The Vendor is responsible for ensuring that the following identifying information appears on the outside of the package:

- “Sealed Cost Offer”
- “Project Name”
- “RFO ID: (Insert Number)”
- “Name and address of Vendor”

If a delivery service is used that prohibits such markings in the outside of the package, this information must be placed in plain view on the outside of an interior envelope or package.

## COST OFFER

Vendors responding to this RFO must be able to grant pricing discounts based on statewide volume or quantity(s). Vendors are responsible to clearly itemize all costs.

**Cost Offers must itemize cost details for scalable factors stated in RFO Section 2.3 as they impact each line item cost. A Cost Offer must be separately completed for each RRMS software type (RMS, JMS and CAD). Vendors offering combined software of any two or more RRMS software type as a packaged solution must complete a separate cost offer for each package solution available.**

- 1 RRMS Project Implementation costs are a one-time cost per local agency for implement, install, test, set-up, etc.
- 2 Existing data migration costs for initial implementation of LEA for any RMS, JMS, or CAD Software product (including software package)
- 3 Post award enhancement / modification – Cost to the customer should the need arise for the RRMS Customers to request a modification or enhancement of standard functionality. Costs must be listed by type of work potentially involved in the performance of the customization / modification and the cost per hour for this type of work.
- 4 RRMS Annual License (Cost per local agency/Customer) per year to utilize the RRMS product/service.
- 5 RRMS Data Training/Documentation costs are one-time costs per local agency for training and/or documentation.
- 6 RRMS Hosting Service (Vendor Hosted) are costs to local agency per year for hosting service(s).
- 7 RRMS Hosting Service (Agency Hosted) are costs to local agency per year for hosting service(s).
- 8 Other RRMS Cost 1 are other costs per local agency not identified as a unique line item in the Cost Offer. All costs must be itemized and specify annual vs. one-time.
- 9 Other RRMS Cost 2 are other costs per local agency not identified as a unique line item in the Cost Offer. All costs must be itemized and specify annual vs. one-time.

- 10 Other RRMS Cost 3 are other costs per local agency not identified as a unique line item in the Cost Offer. All costs must be itemized and specify annual vs. one-time.
- 11 Other RRMS Cost 4 are other costs per local agency not identified as a unique line item in the Cost Offer. All costs must be itemized and specify annual vs. one-time.

<b>1. RRMS Project Implementation</b>	
Size 1 = ≥51	
Size 2 = 26 to 50	
Size 3 = 11 to 25	
Size 4 = ≤10	
Other	
<b>2. Existing Data Migration</b>	
List factor for pricing = _____	
List factor for pricing = _____	
List factor for pricing = _____	
<b>3. Enhancements and Modifications</b>	
Cost per hour - Development type= _____	
Cost per hour - Development type= _____	
Cost per hour - Development type= _____	
Cost per hour - Development type= _____	
<b>4. RRMS Annual License</b>	
Size 1 = ≥51	
Size 2 = 26 to 50	
Size 3 = 11 to 25	
Size 4 = ≤10	
Other	
<b>5. RRMS Data Training/Documentation</b>	
Size 1 = ≥51	
Size 2 = 26 to 50	
Size 3 = 11 to 25	
Size 4 = ≤10	
Other	

<b>6. RRMS Hosting Service (Vendor Hosted)</b>	
Cost per month	
Cost per year	
Other	
<b>7. RRMS Hosting Service (Customer Hosted)</b>	
Cost per month	
Cost per year	
Other	
<b>8. Other RRMS Cost 1</b>	
Please describe:	
<b>9. Other RRMS Cost 2</b>	
Please describe:	
<b>10. Other RRMS Cost 3</b>	
Please describe:	
<b>11. Other RRMS Cost 4</b>	
Please describe:	

**The Cost Offer must be signed, labeled, then bound and sealed separately from the Technical Offer. Any Offers that do not clearly and accurately itemize each cost could be cause for rejection.**

\_\_\_\_\_  
 (Authorized Signature of Entity Official)

\_\_\_\_\_  
 Printed Name

\_\_\_\_\_  
 Title

\_\_\_\_\_  
 Name of Entity

**APPENDIX B**

**TXDPS RRMS RFO  
VENDOR INFORMATION  
(Must sign and submit with Offer)**

**VENDOR INFORMATION**  
**YOU MUST COMPLETE THE FOLLOWING:**

\* **TAX NO.** \_\_\_\_\_  
The Texas ID Number is the taxpayer number assigned and used by the Comptroller of Public Accounts of Texas.

\* **VENDOR NAME:** \_\_\_\_\_

\* **VENDOR MAILING ADDRESS** \_\_\_\_\_

\***VENDOR MAILING CITY** \_\_\_\_\_ \***STATE** \_\_\_\_\_ \***ZIP** \_\_\_\_\_

\***VENDOR CONTACT PERSON:** \_\_\_\_\_

\_\_\_\_\_  
\* (AUTHORIZED SIGNATURE)

**FAILURE TO SIGN WILL DISQUALIFY OFFER (AUTHORIZED SIGNATURE)**

\*PHONE NUMBER: \_\_\_\_\_ \*FAX NUMBER: \_\_\_\_\_

\*E-MAIL: \_\_\_\_\_

\*REQUIRED must be filled out completely

Please use additional page(s) to list name and location of major offices and other facilities that must be used as part of the Vendor's performance under the terms of this RFO.

When mailing or hand delivering your Offer, please place a label in the lower left-hand corner of the sealed mailing envelope or box; If Offer requires more than one envelope or box, place a label on each sealed envelope or box. Below is the example of the format:

Courier Delivery:  
Texas Department of Public Safety  
Accounting and Budget Control, MSC 0130  
Attn: Alfred Ramos  
5805 North Lamar Blvd.  
Austin, TX 78752-0130  
RFO #: 405-IT10-0542  
RFO Closing Date: 06/16/10

Mail To:  
Texas Department of Public Safety  
Accounting and Budget Control, MSC 0130  
Attn: Alfred Ramos  
P.O. Box 4087  
Austin, TX 78773-0130  
RFO #: 405-IT10-0542  
RFO Closing Date: 06/16/10

**APPENDIX C**

**ANTI-LOBBYING AFFIDAVIT  
(Must sign and submit with Offer)**

**Anti-Lobbying Affidavit**

On behalf of the entity named below, I, an official with authority to bind such entity, execute this Affidavit as a part of the entity’s Offer to:

Request for Offer No. 405-IT10-0542

By executing this Affidavit, the entity agrees to the following terms and conditions of this requisition.

From and after the posting of this RFO for the above noted requisition, the entity, its employees, officials, agents and subcontractors, shall not communicate or attempt to communicate about this requisition and the entity’s Offer, with TXDPS personnel, the evaluation committee members and the other TXDPS officials involved in making recommendations or decisions for award of contracts arising from this requisition; provided, however, entity, its employees, officials, agents and subcontractors shall be allowed to participate in the TXDPS sponsored evaluation process, in the form authorized.

Further, the entity shall not, through indirect means of unpaid associates, volunteers or other persons, communicate or attempt to communicate about the entity’s Offer to any TXDPS personnel, the evaluation committee members or other TXDPS officials involved in making recommendations or decisions for award of contracts arising from this requisition. The entity understands and agrees that violation of this Affidavit may result in rejection of its Offer, as a violation of the terms and conditions of the procurement process.

\_\_\_\_\_  
(Authorized Signature of Entity Official)

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Name of Entity

## **APPENDIX D**

### **AFFIRMATION CLAUSES AND PREFERENCES (Must sign and submit with Offer)**

## **Affirmation Clauses**

By signature hereon, the Vendor certifies that:

All statements and information prepared and submitted in the Vendor's Offer to this Request for Offer are current, complete and accurate.

He/she has not given, offered to give, nor intends to give at anytime hereafter, any economic opportunity, future employment, gift, loan gratuity, special discount, trip, favor, or service to a public servant in connection with the submitted Offer.

Signing this Offer with a false statement shall void the submitted Offer or any resulting contracts.

Neither the Vendor or the firm, corporation, partnership, or institution represented by the Vendor or anyone acting for such firm, corporation, or institution has violated the antitrust laws of this State, codified in Section 15.01, et seq., Texas Business and Commerce Code, or the Federal antitrust laws, nor communicated directly or indirectly the offer made to any competitor or any other person engaged in such line of business. By signing this Offer, Vendor certifies that if a Texas address is shown as the address of the Offer, Vendor qualifies as a Texas Bidder as defined in Title 34 TAC Section 20.32(68).

Under Section 2155.004, Government Code, the vendor certifies that the individual or business entity named in this Offer or contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate.

Under Section 231.006 of the Texas Family Code (relating to child support), the individual or business entity named in this solicitation is eligible to receive the specified payment and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate. The Offer includes the names and Social Security Numbers of each person with a minimum of twenty-five percent (25%) ownership of the business entity submitting the Offer. Respondents that have pre-registered this information on the TBPC Centralized Master Bidders List have satisfied this requirement. If not pre-registered, provide the names and Social Security Number with the Offer.

Respondent is in compliance with Texas Government Code, Section 669.003, relating to contracting with an executive of a state agency. If Section 669.003 applies, respondent shall provide the following information as an attachment to this Offer: Name of former executive, name of state agency, date of separation from state agency, position with respondent, and date of employment with respondent.

Respondent certifies that it has not been an employee of the *Texas Department of Public Safety* within the last twelve (12) months.

Respondent agrees that any payments due under this contract will be applied towards any debt, including but not limited to delinquent taxes and child support that is owed to the State of Texas.

Respondent represents and warrants that the individual signing this Offer is authorized to sign this document on behalf of the respondent and to bind the respondent under any contract resulting from this Offer.

*Respondent represents and warrants that they have read and understand the security requirements articulated in the FBI's CJIS Security policy and, if selected as a certified provider, will execute a CJIS Security Addendum in conjunction with the associated RRMS contract.*

Respondent certifies that it and its principals are eligible to participate in this transaction and have not been subjected to suspension, debarment, or similar ineligibility determined by any federal, state or local governmental entity and that Respondent is in compliance with the State of Texas statutes and rules relating to procurement and that Respondent is not listed on the federal government's terrorism watch list as described in Executive Order 13224. Entities ineligible for federal procurement are listed at <http://www.epls.gov>.

"Under Section 2155.006, Government Code, the vendor certifies that the individual or business entity named in this bid or contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate."

"Under Section 2261.053, Government Code, the contractor certifies that the individual or business entity named in this bid or contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate."

### **COMPUTER EQUIPMENT RECYCLING PROGRAM**

Each vendor responding to this RFO must certify the vendor's compliance with Section 361.965(b) of the Health and Safety Code regarding compliance with Subchapter Y (Computer Equipment Recycling Program) of Chapter 361 of the Health and Safety Code. Failure to provide this certification renders the prospective bidder ineligible to participate in the bidding.

### **PREFERENCES:**

See Section 2.38 of the State of Texas Procurement Manual regarding preferences. Check below to claim a preference under 34 TAC Rule 20.38

- Goods produced or offered by a Texas bidder that is owned by a Texas resident service-disabled veteran

- Goods produced in Texas or offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
- Agricultural products grown in Texas
- Agricultural products offered by a Texas bidder
- Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
- Services offered by a Texas bidder that is not owned by a Texas resident service disabled veteran
- Texas Vegetation Native to the Region
- USA produced supplies, materials or equipment
- Products of persons with mental or physical disabilities
- Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel
- Energy Efficient Products
- Rubberized asphalt paving material
- Recycled motor oil and lubricants
- Products produced at facilities located on formerly contaminated property
- Products and services from economically depressed or blighted areas
- Vendors that meet or exceed air quality standards
- Recycled or Reused Computer Equipment of Other Manufacturers
- Foods of Higher Nutritional Value

---

Signature

---

Date

---

Printed Name

---

Title

## APPENDIX E

### **HUB SUBCONTRACTING PLAN (HSP) (Must sign and submit with Offer)**

Must be completed, signed and returned with the Offer. Include all subcontractors on the HSP, and whether they are a HUB firm or not. Complete the remainder of the forms. Failure to do so will render the Offer incomplete and it will be rejected.

Offer Package # 2, posted separately to the ESBD, provides instructions to assist with finding Historically Underutilized Businesses on the State of Texas CMBL to be used when preparing the HSP.

If further assistance is needed in preparing the HSP, you may contact the DPS HUB Liaison Julia Hummel at (512) 424-7346.

TPASS has posted an MP3 Audio/Video file (with additional text version available) that reviews the HSP by section and gives clear direction in properly completing the HSP.

The MP3 file is located at the following link:

<http://www.cpa.state.tx.us/procurement/prog/hub/hub-forms/>

## **APPENDIX F**

### **NON-DISCLOSURE AGREEMENT REGARDING SENSITIVE INFORMATION**

**Vendor must submit to TXDPS a signed Non-Disclosure Agreement to  
obtain Appendices G and L**

**NONDISCLOSURE AGREEMENT WITH TEXAS  
DEPARTMENT OF PUBLIC SAFETY  
REGARDING SENSITIVE OR ACQUISITION INFORMATION**

TO: PARTIES RECEIVING SENSITIVE DOCUMENTS ASSOCIATED WITH  
REQUEST FOR OFFER #405-IT10-0542

FROM: TEXAS DEPARTMENT OF PUBLIC SAFETY (TXDPS)

SUBJECT: Certification Regarding Non-disclosure of Sensitive or Acquisition  
Information; Specifically, Appendix G

The proper custody, use, and preservation of official state and national information related to procurements cannot be overemphasized. It is essential that all personnel associated with acquisitions, including respondents, to a request for Offer, strictly comply with the applicable provisions of policy, law and regulation. In order to protect the criminal justice security required for the Federal Bureau of Investigation (FBI) and the National Law Enforcement Telecommunications (NLETS) systems, TXDPS requires that you execute the following certification prior to receipt of the above cited documents.

Please reproduce this agreement and have it signed by every employee who will have access to the above-cited Appendices. Return all signed non-disclosure agreements to TXDPS prior to requesting the Appendices. Multiple copies of the Appendices will be provided from the TXDPS to any vendor, not to exceed the number of non-disclosure agreements received from that vendor.

I understand that unless otherwise authorized, the release of above-cited Appendices or information concerning the documents shall be at the sole discretion and direction of the TXDPS, consistent with the policies of the FBI, NLETS, and applicable laws and regulations.

*I will not disclose or otherwise release the documents to anyone other than the following: a) the TXDPS; and, b) employees or subcontractors of the vendor associated with preparation of an Offer with the TXDPS who have a need to see the documents and who have executed this nondisclosure agreement and forwarded it to the TXDPS.*

*I will use the above Appendices only for the purpose of preparing a response to the TXDPS Request for this RFO.*

*I will not make a copy through any medium of any part of these Appendices. I will return the original of these Appendices to the TXDPS with my company's written Offer.*

If, upon review of the Request for Offer, my company elects not to respond, I will return all copies of the above-cited Appendices to the TXDPS on or before the deadline stated in Section 3.2 Schedule.

*I am aware that the unauthorized use or disclosure of these documents may subject me and/or my company to criminal, civil, and/or administrative penalties.*

*If, for any reason, the above cited Appendices are released from my custody or are provided to or accessed by a person who has not signed this agreement, I will provide written notice to the contact and address provided in Appendix A. This notice must be provided within two days of the event and will contain a detailed written description of the event.*

*I understand that this certification remains in effect until I return the original copies of the above-cited Appendices to the TXDPS at the address identified in the requisition.*

This agreement is governed by Texas law and the venue for any litigation shall be Travis County, Texas, in a court of competent jurisdiction.

In order to receive the above-cited documents you must first provide the TXDPS with a copy of this non-disclosure agreement containing an original signature of a person who requires access to the documents. Any questions regarding the proper handling of information in this project should be addressed to the contact provided in Appendix A.

I have read and fully understand this non-disclosure agreement with the TXDPS. I am legally competent to execute this contract and I do so of my own free will and accord, without reliance on any representation of any kind or character by the TXDPS that is not expressly set forth herein. I understand that I have the opportunity to consult with a lawyer prior to signing this agreement. I will comply with this agreement.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Company Name: \_\_\_\_\_

## **APPENDIX G**

### **FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES CJIS SECURITY POLICY PACKET**

**The CJIS Security Policy Packet may only be obtained by submitting a signed Non-Disclosure Agreement (Appendix F) directly to the purchaser. It is the responsibility of the vendor to notify TXDPS purchaser of preference of receipt: facsimile, mail, hardcopy or electronically. Vendor must submit an originally signed CJIS Security Addendum Certification for each employee performing duties related to this project prior to final contract execution. Each original Certification must include an original signature of the employee and a vendor (contractor) representative. Non-compliance by vendor will be cause for vendor disqualification. The Vendor MUST sign and submit the CJIS Policy documents with Offer)**

**APPENDIX H**

**TEXAS GOVERNMENT CODE  
DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION**

Sec. 411.083. DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION.

(a) Criminal history record information maintained by the department is confidential information for the use of the department and, except as provided by this subchapter, may not be disseminated by the department.

- (b) The department shall grant access to criminal history record information to:
- (1) criminal justice agencies;
  - (2) noncriminal justice agencies authorized by federal statute or executive order or by state statute to receive criminal history record information;
  - (3) the person who is the subject of the criminal history record information;
  - (4) a person working on a research or statistical project that:
    - (A) is funded in whole or in part by state funds; or
    - (B) meets the requirements of Part 22, Title 28, Code of Federal Regulations, and is approved by the department;
  - (5) an individual or an agency that has a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice under that agreement, if the agreement:
    - (A) specifically authorizes access to information;
    - (B) limits the use of information to the purposes for which it is given;
    - (C) ensures the security and confidentiality of the information; and
    - (D) provides for sanctions if a requirement imposed under Paragraph (A), (B), or (C) is violated;
  - (6) an individual or an agency that has a specific agreement with a noncriminal justice agency to provide services related to the use of criminal history record information disseminated under this subchapter, if the agreement:
    - (A) specifically authorizes access to information;
    - (B) limits the use of information to the purposes for which it is given;
    - (C) ensures the security and confidentiality of the information; and
    - (D) provides for sanctions if a requirement imposed under Paragraph (A), (B), or (C) is violated;
  - (7) a county or district clerk's office; and
  - (8) the Office of Court Administration of the Texas Judicial System.

(c) The department may disseminate criminal history record information under Subsection (b)(1) only for a criminal justice purpose. The department may disseminate criminal history record information under Subsection (b)(2) only for a purpose specified in the statute or order. The department may disseminate criminal history record information under Subsection (b)(4), (5), or (6) only for a purpose approved by the department and only under rules adopted by the department. The department may disseminate criminal history record information under Subsection (b)(7) only to the extent necessary for a county or district clerk to perform a duty imposed by law to collect and report criminal court disposition information. Criminal history record information disseminated to a clerk under Subsection (b)(7) may be used by the clerk only to ensure that information reported by the clerk to the department is accurate and complete. The dissemination of information to a clerk under Subsection (b)(7) does not affect the authority of the clerk to disclose or use information submitted by the clerk to

the department. The department may disseminate criminal history record information under Subsection (b)(8) only to the extent necessary for the office of court administration to perform a duty imposed by law to compile court statistics or prepare reports. The office of court administration may disclose criminal history record information obtained from the department under Subsection (b)(8) in a statistic compiled by the office or a report prepared by the office, but only in a manner that does not identify the person who is the subject of the information.

(d) The department is not required to release or disclose criminal history record information to any person that is not in compliance with rules adopted by the department under this subchapter or rules adopted by the Federal Bureau of Investigation that relate to the dissemination or use of criminal history record information.

**Sec. 411.084. USE OF CRIMINAL HISTORY RECORD INFORMATION.**

(a) Criminal history record information obtained from the department under this subchapter:

- (1) is for the exclusive use of the authorized recipient of the information; and
- (2) may be disclosed or used by the recipient only if, and only to the extent that, disclosure or use is authorized or directed by:
  - (A) this subchapter;
  - (B) another statute;
  - (C) a rule adopted under a statute; or
  - (D) an order of a court of competent jurisdiction.

(b) Notwithstanding Subsection (a) or any other provision in this subchapter, criminal history record information obtained from the Federal Bureau of Investigation may be released or disclosed only to a governmental entity or as authorized by federal statute, federal rule, or federal executive order.

**Sec. 411.085. UNAUTHORIZED OBTAINING, USE, OR DISCLOSURE OF CRIMINAL HISTORY RECORD INFORMATION; PENALTY.**

(a) A person commits an offense if the person knowingly or intentionally:

- (1) obtains criminal history record information in an unauthorized manner, uses the information for an unauthorized purpose, or discloses the information to a person who is not entitled to the information; or
- (2) violates a rule of the department adopted under this subchapter.

(b) An offense under Subsection (a) is a Class B misdemeanor, except as provided by Subsection (c).

(c) An offense under Subsection (a) is a felony of the second degree if the person:

- (1) obtains, uses, or discloses criminal history record information for remuneration or for the promise of remuneration; or

(2) employs another person to obtain, use, or disclose criminal history record information for remuneration or for the promise of remuneration.

(d) The department shall provide a copy of this section to:

- (1) each person who applies for access to criminal history record information maintained by the department; and
- (2) each private entity that purchases criminal history record information from the department.

**APPENDIX I**

**SECTION 1.01  
CODE OF FEDERAL REGULATIONS  
TITLE 28, PART 20**

CODE OF FEDERAL REGULATIONS  
TITLE 28--JUDICIAL ADMINISTRATION  
CHAPTER I--DEPARTMENT OF JUSTICE  
PART 20--CRIMINAL JUSTICE INFORMATION SYSTEMS  
Subpart A--General Provisions

Sec. 20.3 Definitions. As used in these regulations:

(a) Act means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701, et seq., as amended.

(b) Administration of criminal justice means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(c) Control Terminal Agency means a duly authorized state, foreign, or international criminal justice agency with direct access to the National Crime Information Center telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

(d) Criminal history record information means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

(e) Criminal history record information system means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of criminal history record information.

(f) Criminal history record repository means the state agency designated by the governor or other appropriate executive official or the legislature to perform centralized recordkeeping functions for criminal history records and services in the state.

(g) Criminal justice agency means:

(1) Courts; and

(2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included.

(h) Direct access means having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

(i) Disposition means information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall [[Page 391]] include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial- defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(j) Executive order means an order of the President of the United States or the Chief Executive of a state that has the force of law and that is published in a manner permitting regular public access.

(k) Federal Service Coordinator means a non-Control Terminal Agency that has a direct telecommunications line to the National Crime Information Center network.

(l) Fingerprint Identification Records System or "FIRS" means the following FBI records: Criminal fingerprints and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities; civil fingerprints submitted by federal agencies and civil fingerprints submitted by persons desiring to have their fingerprints placed on record for personal identification purposes; identification records, sometimes referred to as "rap sheets," which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the FIRS; and a name index pertaining to all individuals whose fingerprints are maintained in the FIRS. See the FIRS Privacy Act System Notice periodically published in the Federal Register for further details.

(m) Interstate Identification Index System or "III System" means the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

(n) National Crime Information Center or "NCIC" means the computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the

United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information. The NCIC includes, but is not limited to, information in the III System. See the NCIC Privacy Act System Notice periodically published in the Federal Register for further details.

(o) National Fingerprint File or ``NFF" means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(p) National Identification Index or ``NII" means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(q) Nonconviction data means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; information disclosing that the police have elected not to refer a matter to a prosecutor, that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed; and information that there has been an acquittal or a dismissal.

(r) State means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(s) Statute means an Act of Congress or of a state legislature or a provision of the Constitution of the United States or of a state.

**APPENDIX J**

**TXDPS CONTRACT  
REMOTELY HOSTED CRIMINAL INCIDENT  
RECORDS MANAGEMENT SYSTEM  
(RRMS)**

**CONTRACT FOR  
TXDPS REMOTE CRIMINAL RECORDS MANAGEMENT SYSTEM**

**I. PARTIES**

This contract ("Contract" or "Agreement") is made and entered into by and between \_\_\_\_\_ ("Contractor" or "Vendor") and the Department of Public Safety, an agency of the State of Texas, ("TXDPS"), pursuant to Request for Offer No. 405-\_\_\_\_\_. Contractor and TXDPS are collectively referred to in this Contract as the "Parties."

WHEREAS, on the basis of the written representations contained in Contractor's Offer, as well as Contractor's presentation, discussions with Contractor and Contractor's experience relating to the deliverables contemplated by this Contract, TXDPS desires to engage Contractor to provide the deliverables on the terms and conditions as stated herein;

WHEREAS, Contractor has represented to TXDPS that Contractor is a leader in and has extensive experience in providing the deliverables for this Contract;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, Contractor and TXDPS hereby covenant and agree as follows:

**II. TERMS AND CONDITIONS**

**1. Controlling Order of Contract**

This Contract between TXDPS and Contractor consists of the documents listed below. In the event of any conflicts between the documents, the documents will control in the following order of precedence:

The following Contract documents:

- i. This Contract, including any appendices
- ii. TXDPS Request for Offers as posted, including all attachments or appendices, however Appendix J (Attached Contract) is deleted
- iii. Contractor's original Offer as submitted, including all appendices
- iv. Schedule and the Statements of Work, as defined in Section III herein
- v. TXDPS Purchase Order, including any Purchase Order Change Notices and excluding any pre-printed terms and conditions.

**2. Contract Term**

This contract shall become effective on the date it is signed by the last of the two parties to this contract. The initial term of this contract shall last for two (2) years after execution of this contract. TXDPS reserves the right to renew this Agreement, in whole or in part under the same terms and conditions, for up to six (6) years in increments of up to two (2) years each. In no case shall the full term of the contract including extensions exceed eight (8) years. TXDPS will exercise this option by providing written notice to the Contractor prior to the expiration of this Agreement. Any renewal will only become effective after both Parties sign a document to renew this Agreement.

In addition to the rights granted to TXDPS above, TXDPS also has the right, at its own election, to extend the Contract for ninety (90) days beyond the expiration of any initial or renewal term. TXDPS will exercise this unilateral right by providing notice to the Contractor before the end of any initial or renewal term of the Contract without the necessity of the Contractor's approval or signature. Vendor shall warrant all deliverables under this contract to be free of defects as defined in Section 51.2.

### **3. Modification of Contract Terms and/or Amendments**

The terms and conditions of the Contract shall govern all transactions by local law enforcement agencies (LEAs) under the Contract. The Contract may only be modified or amended upon mutual written agreement of TXDPS and Vendor.

LEAs shall not have the authority to modify the terms of the Contract; however, additional LEA terms and conditions which do not conflict with the Contract and are acceptable to Vendor may be added to the LEA Purchase Order. No additional term or condition added to a Purchase Order issued by the LEA may weaken any term or condition of the RRMS Contract. Pre-printed terms and conditions on any Purchase Order issued will have no force and effect. In the event of a conflict between a Purchase Order and the RRMS Contract, the RRMS Contract term or condition shall control.

### **4. Submitting TXDPS Invoices and Receiving Payment / Acceptance Process**

TXDPS will pay Contractor on the basis of itemized invoices submitted to and approved by TXDPS, showing the actual deliverables provided and the attendant charge. Itemized invoices must clearly identify the project phase or title, deliverables delivered, the number of hours that each allocated employee worked and the date range of work performed for the associated charge. Chapter 2251 of the Texas Government Code shall govern payment and accrual of interest on any overdue payments.

Invoices must also include the TXDPS Purchase Order number, Contractor's Texas Identification Number System (TINS) number, Contractor's address, Contractor's contact person and Contractor's phone number. All invoices must be mailed to:

CRIME RECORDS SERVICE  
TEXAS DEPARTMENT OF PUBLIC SAFETY  
ATTENTION: Desiree Taylor  
PO BOX 4087  
AUSTIN, TX 78773

The State will not incur any penalty for late payment if the invoice was not mailed to the appropriate address identified herein.

If TXDPS, for any reason, including lack of supporting documentation, disputes any items in any invoices submitted by Contractor, TXDPS shall temporarily delete the disputed items and pay the remaining amount of the invoice. TXDPS will timely notify

Contractor of the dispute and may request clarification and/or remedial action. If the dispute is resolved in the Contractor's favor, TXDPS will pay remaining portion of the original invoice in accordance with the Prompt Payment Act, Chapter 2251 of the Texas Government Code. If the dispute is resolved in TXDPS' favor, the Contractor shall resubmit an invoice reflecting all corrections. TXDPS will not be responsible for reimbursements due to travel and per diem expenses.

#### **4.1 Vendor Invoices for Deliverables**

TXDPS and/or LEA will only accept a properly prepared invoice as defined in Section 4 for payment after the acceptance for each deliverable as defined in the Section herein entitled "Final Operating Capability". Deliverables are defined as those services (excluding those services defined as reoccurring operational services in Section 4.2) or products procured through this Contract, including but not limited to:

- Implementation
- Migration
- Enhancements
- Modifications
- Product Upgrades

#### **4.2 Vendor Invoices for Reoccurring Operational Service Expenses**

TXDPS and/or LEA will accept a properly prepared invoice as defined in Section 4 for payment of reoccurring operational service expenses at the beginning of the service period. RRMS reoccurring operational service expenses include but are not limited to:

- Licensing Cost
- Hosting Services
- Other Annual expenses to maintain or support the RRMS

### **5. Compliance with Permitting and Purchasing Laws**

Contractor must be in compliance with any and all applicable permitting and purchasing laws that Texas state agencies must address before conducting business with a vendor. Contractor agrees that payments under this Contract must be applied towards any of Contractor's debts to the State of Texas, including, but not limited to any child support or delinquent taxes, until paid in full.

### **6. Compliance with State, Federal, and Local Laws, Rules and Regulations**

Contractor must comply with all applicable state, federal and local laws and ordinances in providing deliverables to TXDPS or the LEA under this Contract. Without limiting the generality of the foregoing, Contractor must be able to demonstrate compliance with the Federal Tax Reform Act of 1986, Section 1706, amending Section 530 of the Revenue Act of 1978, dealing with issuance of W-2s to common law employees. Contractor is responsible for both federal and state unemployment insurance coverage and standard workers' compensation insurance coverage. Contractor must comply with all federal and state tax laws and withholding requirements. TXDPS or LEA will not be liable to Contractor/subcontractor(s) or its employees for any unemployment insurance or

workers' compensation coverage or federal or state tax withholding requirements. Contractor may be required to demonstrate compliance with such laws at the written request of TXDPS or LEA.

Contractor shall provide all labor and equipment necessary to furnish the deliverables under this Contract. All employees of Contractor shall be a minimum of 17 years of age and experienced in the type of work to be performed. Absent prior, written permission from TXDPS or LEAs, no visitors or relatives of Contractor's employees and subcontractors will be allowed on TXDPS or LEAs property unless they are bona fide employees or subcontractors of Contractor performing work under this Contract.

Contractor agrees that at all times its personnel must observe and comply with all laws, regulations and rules pertaining to state facilities, including but not limited to parking and security regulations. Additionally, Contractor personnel must agree to and comply with all relevant TXDPS or LEA policies that relate to the security of data and confidentiality of information.

In the event that any of Contractor's personnel has failed to comply with such laws, regulations or rules, TXDPS or LEA will have the right to require Contractor to remove such person from any involvement in this Contract.

#### **7. Conflict of Law, Choice of Law, U.N. Convention on Contracts and Venue**

This Contract shall be governed by the substantive and procedural laws of the State of Texas. The following shall not apply to this Contract: a) the conflicts of law principles and rules of Texas and any other jurisdiction; and b) the United Nations Convention on Contracts for the International Sale of Goods.

Except as provided by Chapter 2260 of the Texas Government Code and the State Office of Administrative Hearings' administrative rules, venue for any litigation or contract claims shall be in the State Office of Administrative Hearings or a court of competent jurisdiction in Travis County, Texas.

#### **8. Force Majeure**

Neither Contractor, LEA nor TXDPS shall be liable to the other for any delay in performance of, or failure to perform, any obligation contained herein caused by *force majeure*, provided the party seeking to be excused has prudently and promptly acted to take any and all reasonable corrective measures that are within such party's control; and provided, further, that any action or inaction by a subcontractor of a party shall not be considered to be outside the control of such party except to the extent the Parties may expressly agree otherwise in this Contract. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been corrected.

*Force majeure* is defined as those causes beyond the control of the party required to perform that are generally recognized under Texas law as a *force majeure* event, such as acts of God, acts of war, epidemic and court orders. Contractor shall immediately

upon discovery notify the TXDPS PM and LEA PM in writing of any delays in the implementation schedule or the delivery of deliverables without regard to responsibility, fault or negligence.

### **9. Severability**

If one or more provisions of this Contract, or the application of any provision to any party or circumstance, is held invalid, unenforceable, or illegal in any respect by a final order/judgment of the State Office of Administrative Hearings or a court of competent jurisdiction, the remainder of this Contract and the application of the provision to other parties or circumstances will remain valid and in full force and effect.

### **10. Survival**

Any provisions of this Contract that impose continuing obligations on the Parties including, but not limited to the following, will survive the expiration or termination of this Contract for any reason:

- a. The indemnity obligations,
- b. Contractor's news release, advertisement and publicity restrictions,
- c. Ownership rights,
- d. Recordkeeping requirements and audit rights,
- e. Warranty,
- f. Confidentiality and security obligations, including the FBI CJIS Security Addendum as it now exists and as it may thereafter be amended,
- g. And any other provisions of this Contract that impose continuing obligations on either of the Parties or that govern the rights and limitations of either of the Parties after the expiration or termination of this Contract.

### **11. Non-Waiver of Defaults**

Any failure of TXDPS, at any time, to enforce or require the strict keeping and performance of any provision of this Contract will not constitute a waiver of such provision, and will not affect or impair same or the right of TXDPS at any time to avail itself of same. A waiver does not become effective unless TXDPS expressly agrees to such waiver in writing. Any acceptance, payment or use by TXDPS regarding any deliverable provided shall not constitute a waiver or otherwise impair or prejudice any right, power, privilege or remedy available to TXDPS to enforce its rights, as such rights, powers, privileges and remedies are specifically preserved.

### **12. No Liability for Employees and Officers**

Each party to this Contract shall have no liability whatsoever for the actions or omissions of an individual employed by another party, regardless of where the individual's actions or omissions occurred. Each party is solely responsible for the actions and/or omissions of its employees and officers; however, such responsibility is only to the extent required by Texas law. Where injury or property damage result from the joint or concurring negligence of the Parties, liability, if any, shall be shared by each party in accordance with the applicable laws of the State of Texas, subject to all defenses, including governmental immunity. These provisions are solely for the benefit

of the Parties hereto and not for the benefit of any person or entity not a party hereto; nor shall any provision hereof be deemed a waiver of any defenses available by law.

### **13. Legislative Action**

TXDPS is a state agency whose authority is subject to the actions of the Texas Legislature and the United States Congress. If TXDPS and/or the subject matter of this Contract become subject to a legislative or regulatory change or the revocation of statutory or regulatory authority that would render the deliverables to be provided under this Contract impossible, unnecessary, void or substantially amended or that would terminate the appropriations for this Contract, TXDPS may immediately terminate this Contract without penalty to, or any liability whatsoever on the part of, TXDPS, the State of Texas and the United States. This Contract does not grant Contractor a franchise or any other vested property right.

Termination under this section is immediate, so TXDPS is not required to provide thirty (30) days notice under this section.

If funding for this Contract is reduced by law or the statutory amount of compensation authorized for the Vendor is reduced, TXDPS may, upon thirty (30) days written notice to the Vendor, reduce the deliverables in such manner and for such periods of time as TXDPS may elect.

### **14. Termination by Default**

In the event that Contractor fails to carry out or comply with any of the requirements of this Contract with TXDPS or the LEA, TXDPS may notify Contractor of such failure or default in writing and demand that the failure or default be remedied within ten (10) days. In the event that Contractor fails to remedy such failure or default within the ten (10) day period, TXDPS will have the right to cancel this contract upon ten (10) days written notice.

The cancellation of this contract, under any circumstances whatsoever, will not affect or relieve Contractor from any liability that may have been incurred pursuant to this Contract, and such cancellation by TXDPS will not limit any other right or remedy available to TXDPS at law or in equity.

### **15. Termination for Cause or Convenience**

This Contract may be terminated as follows:

- For Convenience: This Contract may be terminated, in whole or in part without penalty, by TXDPS, without cause by giving thirty (30) days written notice of such termination to Contractor.
- For Cause: This Contract may be terminated by TXDPS if Contractor fails to perform as agreed or is otherwise in default, without the necessity of complying with the requirements in the section herein entitled "Termination by Default."

- For Lack of Funding: This project may be partially or fully funded through a state or federal grant award. Should funds become unavailable for any reason, this contract may be terminated, in whole or in part without penalty, by TXDPS immediately. Should grant funds become unavailable for any reason, this contract may be terminated, in whole or in part by TXDPS immediately, without any obligation to use non-grant funds allocated or appropriated to TXDPS.
- Termination for listing on Federal Excluded Party List, on the Terrorism List (Executive Order 13224) or on the State of Texas Debarred Vendor List: TXDPS shall have the absolute right to terminate this Contract without recourse as follows: a) if Contractor becomes listed on the prohibited vendors list authorized by Executive Order #13224 "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism," published by the United States Department of Treasury, Office of Foreign Assets Control; or b) if Contractor becomes suspended or debarred from doing business with federal government as listed in the Excluded Parties List (EPLS) maintained by the General Services Administration; or c) if the Contractor becomes listed on the State of Texas Debarred Vendor List. TXDPS will provide Contractor with written notice to terminate the contract, which termination will become effective immediately upon Contractor's receipt of the notice.

If Contractor is terminated for cause, TXDPS reserves the right to either re-solicit or re-award the contract to the next best responsive and responsible respondent. The defaulting Contractor will not be considered in the re-solicitation and may not be considered in future solicitations for the same type of work, unless the specification or scope of work significantly changed.

**16. Termination Liability (for Termination for Convenience)**

In no event will termination for convenience by TXDPS give rise to any liability whatsoever on the part of TXDPS whether such claims of Contractor are for compensation for anticipated profits, unabsorbed overhead, interest on borrowing, or for any other reason. TXDPS' sole obligation hereunder is to pay Contractor for deliverables ordered and received prior to the date of termination, if TXDPS accepts such deliverables.

In the event of a termination of the Contract, TXDPS has the option to deduct any pre-paid fees (for recurring deliverables not provided or not provided in compliance with the Contract) from any payments due the Contractor. TXDPS has the right to offset any pre-paid fees payable to TXDPS, as specified above, against any payments due to Contractor. If insufficient payments are available to offset such pre-paid fees, then Contractor shall pay to TXDPS any remaining pre-paid fees within fifteen (15) calendar days following receipt of written notice of the amount due.

**17. No Joint Enterprise**

TXDPS is associated with Contractor only for the purposes and to the extent set forth herein, and with respect to the creation and delivery of deliverables hereunder,

Contractor is and shall be an independent contractor and shall have the sole right to supervise, manage, operate, control, and direct the performance of the details incident to its duties hereunder. Nothing contained herein shall be deemed or construed to create a partnership or joint venture, to create the relationships of an employer-employee or principal-agent, or to otherwise create any liability for TXDPS whatsoever with respect to the indebtedness, liabilities, and obligations of Contractor or any other party.

#### **18. Assignment by the Contractor**

Contractor must not assign or transfer any interest in this Contract without the express, prior written consent of TXDPS.

#### **19. Successors**

This Contract shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors, heirs, administrators, personal representatives, legal representatives and permitted assigns.

#### **20. News Releases, Advertisements and Publicity**

Contractor must not make any news releases, public announcements, or public disclosures, nor will it have any conversations with representatives of the news media, pertaining to this Contract, without the express, prior written approval of TXDPS, and then only in accordance with explicit written instructions from TXDPS.

Contractor must not use the name of the State of Texas or TXDPS in any advertisement, promotion or otherwise for any purpose regarding this Contract without the express prior written consent of TXDPS. TXDPS is not authorized to provide endorsements.

Notwithstanding the foregoing Contractor may make any disclosure required by law or regulation without the approval of TXDPS.

#### **21. Employee Non-Solicitation**

Contractor must not, during the term of this Contract and for a period of twelve (12) months thereafter, solicit for employment any person who is a TXDPS employee or was a TXDPS employee during the previous twelve (12) months with whom Contractor had substantial contact in the course of performing its obligations under this Contract. Indirect solicitations, such as newspaper and internet announcements, are not prohibited by this section.

#### **22. Contract Amendments**

No modification or amendment to this Contract will become valid unless in writing and signed by both Parties. All correspondence regarding modifications or amendments to this Contract must be forwarded to TXDPS for prior review and approval. Only the Executive Director of TXDPS or his/her designee will be authorized to sign changes or amendments.

## **23. Confidentiality and Security Requirements**

### **23.1 General Confidentiality Requirements**

All information provided by TXDPS to Contractor or created by Contractor in performing the obligations under this Contract is confidential and shall not be used by Contractor or disclosed to any person or entity, unless such use or disclosure is required for Contractor to perform work under this Contract.

The obligations of this section do not apply to information that Contractor can demonstrate: (i) is publicly available; (ii) Contractor received from a third party without restriction on disclosure and without breach of contract or other wrongful act; (iii) Contractor independently developed without regard to the TXDPS confidential information; or (iv) is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, provided that Contractor must furnish prompt written notice of such required disclosure and shall reasonably cooperate with TXDPS at TXDPS' cost and expense, in any effort made by TXDPS to seek a protection order or other appropriate protection of its confidential information.

Contractor shall notify TXDPS of any unauthorized release of confidential information within two (2) days of when Contractor knows or should have known of such unauthorized release.

Contractor agrees to maintain all confidential information in confidence during the term of this Contract and after the expiration or earlier termination of this Contract.

If Contractor has any questions or doubts as to whether particular material or information is confidential information, Contractor shall obtain the prior written approval of TXDPS prior to using, disclosing or releasing such information.

Contractor acknowledges that TXDPS' confidential information is unique and valuable, and that TXDPS may have no adequate remedy at law if Contractor does not comply with its confidentiality obligations under this Contract. Therefore, TXDPS shall have the right, in addition to any other rights it may have, to seek in any Travis County court of competent jurisdiction temporary, preliminary and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any confidentiality obligations of Contractor if Contractor fails to perform any of its confidentiality obligations under this Contract.

Contractor shall immediately return to TXDPS all confidential information when this Contract terminates, at such earlier time as when the confidential information is no longer required for the performance of this Contract or when TXDPS requests that such confidential information be returned.

Information, documentation and other material in connection with this Contract, including Contractor's Offer, may be subject to public disclosure pursuant to Chapter 552 of the Texas Government Code.

The FBI and TXDPS have computer security requirements. Contractor's and subcontractor's employees working on this project must sign appropriate agreements and abide by these security requirements, upon TXDPS' request.

### **23.2 Sensitive Personal Information**

To the extent this subsection does not conflict with the subsection herein entitled "General Confidentiality Requirements," Contractor must comply with both subsections. To the extent this subsection conflicts with the subsection herein entitled "General Confidentiality Requirements," this subsection entitled "Sensitive Personal Information" controls.

"Sensitive personal information" is defined as follows:

- (1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - a. Social security number;
  - b. Driver's license number or government-issued identification number; or
  - c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- (2) Information that identifies an individual and relates to:
  - a. The physical or mental health or condition of the individual;
  - b. The provision of health care to the individual; or
  - c. Payment for the provision of health care to the individual.

Sensitive personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

"Breach of system security" is defined as follows": Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information Contractor maintains under this contract, including data that is encrypted if the Contractor's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the Contractor for the purposes of performing under this Contract is not a breach of system security unless the employee or agent of the Contractor uses or discloses the sensitive personal information in an unauthorized manner.

Contractor shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by Contractor under this contract.

Contractor shall notify TXDPS and the affected people of any breach of system security immediately after discovering the breach or receiving notification of the breach, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, Contractor must delay providing notice to the affected people at TXDPS' request if TXDPS determines that the notification will impede a criminal investigation. The notification to the affected people shall be made as soon as TXDPS determines that it will not compromise any criminal investigation.

Contractor must give notice as follows, at Contractor's expense:

- (1) Written notice;
- (2) Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001;
- (3) Notice as follows:
  - a. If Contractor demonstrates that the cost of providing notice would exceed \$250,000, the number of affected people exceeds 500,000, or the Contractor does not have sufficient contact information for the affected people, Contractor may give notice as follows:
    - i. Electronic mail, if the Contractor has an electronic mail address for the affected people;
    - ii. Conspicuous posting of the notice on the Contractor's website;
    - iii. Notice published in or broadcast on major statewide media; or
  - b. If Contractor maintains its own notification procedures (as part of an information security policy for the treatment of sensitive personal information) that comply with the timing requirements for notice under this subsection entitled "Sensitive Personal Information," Contractor may provide notice in accordance with that policy.

If this subsection requires Contractor to notify at one time more than 10,000 people of a breach of system security, the Contractor shall also notify, without unreasonable delay, all each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

### **23.3 Breach of System Security Audit**

TXDPS will retain sole discretion for determining whether the sensitive personal information was reasonably believed to have been acquired by an unauthorized person.

### **23.4 Vendor Consequences for Breach of System Security**

In the event of a breach of system security, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, TXDPS is authorized to assess liquidated damages in the amount of \$1,024 per day for up to sixty (60) days against Contractor. This amount is a reasonable estimate of the damages TXDPS will suffer as a result of such breach and is enforceable. Contractor shall not be responsible and liquidated damages may not be assessed due to a breach of system security caused entirely by someone other than Contractor, Contractor's subcontractor, or Contractor's agent. Any liquidated damages assessed under this contract may, at

TXDPS' option, be deducted from any payments due the Contractor. TXDPS has the right to offset any liquidated damages payable to TXDPS, as specified above, against any payments due to Contractor. If insufficient payments are available to offset such liquidated damages, then Contractor shall pay to TXDPS any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

### **23.5 Termination of Contract for Breach of System Security**

The contract may be terminated by TXDPS if Vendor fails to perform as agreed or is otherwise in default if it was determined the **Vendor** was responsible for a breach of system security and failed to comply with Section 23.1 and 23.2.

### **23.6 Contract Performance Reporting**

TXDPS submits Vendor Performance Forms (VPF) for any purchase over \$25,000. If it was determined the Vendor was responsible for the breach of system security, the VPF for this contract may be submitted with an unsatisfactory performance evaluation.

## **24. Right to Audit and Inspect**

### **24.1 Inspect Services and All Other Deliverables**

TXDPS has the right to inspect and test all services and all other deliverables listed in this Contract, to the extent practicable at all times and places during the term of this Contract. TXDPS shall perform inspections and tests in a manner that will not unduly delay the work.

If TXDPS performs inspections or tests on the premises of Contractor or a subcontractor, Contractor shall furnish, and shall require subcontractor(s) to furnish, at no increase to this Contract's price, all reasonable facilities and assistance for the safe and convenient performance of these duties.

If any of the deliverables do not conform to this Contract's requirements, TXDPS may require Contractor to provide the deliverables again in conformity with this Contract's requirements, at no increase in this Contract's amount, in addition to all other legal and equitable remedies.

### **24.2 Audit**

TXDPS reserves the right to audit Contractor's records and documents regarding compliance with this Contract. Contractor is also subject to audit by any other department or agency, including federal agencies, responsible for determining that the Parties have complied with the applicable laws. The Contractor understands that acceptance of state funds under this contract acts as acceptance of the authority of the State Auditor's Office to conduct an audit or investigation in connection with those funds. The Contractor further agrees to cooperate fully with the State Auditor's Office in the conduct of the audit or investigation, including providing all records requested. The Contractor will ensure that this clause concerning the State Auditor's Office's authority to audit state funds and the requirement to cooperate fully with State Auditor's Office is included in any subcontracts it awards. Additionally, the State Auditor's Office shall at

any time have access to and the rights to examine, audit, excerpt, and transcribe any pertinent books, documents, working papers, and records of the Contractor relating to this contract.

Except as stated otherwise in the section herein entitled "Confidentiality and Security Requirements" or in the CJIS Documents, Contractor must keep all records and documents regarding this Contract for the term of this contract and for four (4) years after the termination of this Contract.

In the event such an audit by TXDPS reveals any errors by TXDPS or the Contractor, the Contractor shall refund TXDPS the full amount of such overpayments within thirty (30) days of such audit findings, or TXDPS at its option reserves the right to deduct such amounts owing TXDPS from any payments due Contractor.

### **25. Ownership of Hardware, Data and Images**

Any hardware delivered by Contractor in the performance of its obligations (if applicable) under this Contract shall be the exclusive property of the Contractor.

TXDPS, Customer or the contributing LEA of the records owns all data and images that are recorded, transmitted, housed or stored through the RRMS. All data and images recorded, transmitted housed or stored (including any converted historical data) by or through the RRMS **MUST** be returned electronically in a format acceptable to the Customer or contributing LEA should the contract expire, be terminated, cancelled, or not renewed for any reason.

### **26. Time is of the Essence**

Time is of the essence for delivering the deliverables as set forth in this Contract.

### **27. Chapter 2260, Texas Government Code**

To the extent Chapter 2260 of the Texas Government Code applies to the contract claim at issue, Contractor must use the dispute resolution process provided for in Chapter 2260 of the Texas Government Code and the applicable TXDPS administrative rules to attempt to resolve all contract claims arising under this Contract.

### **28. Antitrust**

Contractor hereby assigns to TXDPS any and all claims for overcharges associated with this Contract arising under the antitrust laws of the United States 15 U.S.C.A. Section 1, *et seq.* (1973), and the antitrust laws of the State of Texas, Texas Business and Commerce Code Section 15.01, *et seq.* (1967).

### **29. Indemnity**

**CONTRACTOR SHALL INDEMNIFY, DEFEND AND HOLD TXDPS AND THE STATE OF TEXAS (INCLUDING ITS DIRECTORS, EMPLOYEES, AGENTS AND THEIR SUCCESSORS) HARMLESS FROM AND AGAINST ANY OF THE FOLLOWING THAT ARISE OUT OF OR RESULT FROM CONTRACTOR'S NEGLIGENCE (ANY AND ALL), FAULT, ACT, FAILURE TO ACT, OMISSION, BREACH OF THIS**

**CONTRACT OR VIOLATION OF ANY STATE OR FEDERAL LAW AND/OR REGULATION, AS WELL AS ANY VIOLATION OF ANY MATTER MADE THE BASIS OF A TREATY AND/OR CONVENTION AND/OR AGREEMENT BETWEEN THE UNITED STATES AND ANOTHER NATION: CLAIMS; LAWSUITS; DAMAGES; LIABILITIES; PENALTIES; TAXES; FINES; INTEREST; EXPENSES (INCLUDING, WITHOUT LIMITATION, ATTORNEYS' FEES, COURT COSTS, INVESTIGATION COSTS AND ALL DIRECT OR INDIRECT COSTS OR EXPENSES INCURRED IN DEFENDING AGAINST ANY CLAIM, LAWSUIT OR OTHER PROCEEDING, INCLUDING THOSE EXPENSES INCURRED IN ANY NEGOTIATION, SETTLEMENT OR ALTERNATIVE DISPUTE RESOLUTION); ANY AND ALL DAMAGES, HOWEVER CHARACTERIZED, SUCH AS DIRECT, GENERAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES OF ANY KIND (INCLUDING LOST REVENUES OR PROFITS, LOSS OF BUSINESS, LOSS OF USE OR LOSS OF DATA) ARISING OUT OF OR IN CONNECTION WITH OR RELATED TO THIS CONTRACT OR THE RIGHTS PROVIDED THEREIN.**

**IN ANY AND ALL CLAIMS AGAINST TXDPS AND THE STATE OF TEXAS (INCLUDING ITS DIRECTORS, EMPLOYEES, AGENTS AND THEIR SUCCESSORS), BY ANY EMPLOYEE OF THE CONTRACTOR OR ANY EMPLOYEE OF ITS SUBCONTRACTOR(S), THE INDEMNIFICATION OBLIGATION UNDER THIS CONTRACT WILL NOT BE LIMITED IN ANY WAY BY THE AMOUNT OR TYPE OF DAMAGES, COMPENSATION, OR BENEFITS PAYABLE BY OR FOR THE CONTRACTOR OR ANY OF ITS SUBCONTRACTOR(S) UNDER WORKER'S DISABILITY COMPENSATION ACTS, DISABILITY BENEFITS ACTS, OR OTHER EMPLOYEE BENEFITS ACTS.**

**CONTRACTOR'S OBLIGATIONS IN THIS SECTION INCLUDE, BUT ARE NOT LIMITED TO, CLAIMS, LAWSUITS, DAMAGES, ETC. BASED ON A CLAIM THAT ANY PIECE OF EQUIPMENT, GOODS, SOFTWARE, DOCUMENTATION, SERVICES OR OTHER DELIVERABLES SUPPLIED BY CONTRACTOR OR ITS SUBCONTRACTORS, OR THE USE, DISPLAY, OPERATION OR REPRODUCTION THEREOF, INFRINGES ANY UNITED STATES OR FOREIGN PATENT, COPYRIGHT, TRADE SECRET, OR OTHER INTELLECTUAL OR PROPRIETARY RIGHT OF ANY PERSON OR ENTITY. SHOULD THE PIECE OF EQUIPMENT, GOODS, SOFTWARE, ETC. BECOME, OR IN THE CONTRACTOR'S OPINION BE LIKELY TO BECOME, THE SUBJECT OF A CLAIM OF INFRINGEMENT, THE CONTRACTOR, AT ITS OWN EXPENSE, MUST: 1) PROCURE FOR TXDPS THE RIGHT TO CONTINUE USING THE EQUIPMENT, SOFTWARE, GOODS, ETC.; OR 2) IF SUCH OPTION IS NOT REASONABLY AVAILABLE TO CONTRACTOR, CONTRACTOR MUST REPLACE OR MODIFY THE SAME WITH EQUIPMENT, SOFTWARE, GOODS, ETC. OF EQUIVALENT FUNCTION AND PERFORMANCE SO THAT IT BECOMES NON-INFRINGEMENT.**

**THIS SECTION SHALL SURVIVE THE TERMINATION OR EXPIRATION OF THIS CONTRACT.**

### **30. Buy Texas Clause**

Pursuant to Section 2155.4441 of the Texas Government Code, Contractor shall buy Texas products and materials for use in creating and delivering the services authorized in this Contract when such products and materials are available at a comparable price and in a comparable period of time when compared to non-Texas products and materials.

### **31. Family Law Code**

Under Section 231.006, Family Code, Contractor certifies that the individual or business entity named in this Contract is not ineligible to receive the specified payment and acknowledges that this Contract may be terminated and payment may be withheld if this certification is inaccurate.

### **32. Commencement of Work**

Any work performed before final execution of this Contract must be at Contractor's risk and will not be reimbursed.

### **33. Rolling Estoppel**

TXDPS will be conclusively deemed to have fulfilled its obligations under this Contract, unless TXDPS receives a deficiency report from Contractor within five (5) business days of the occurrence of the alleged deficiencies and Contractor identifies specific deficiencies in TXDPS' fulfillment of its obligations in that report. Deficiencies must be described in terms of how they have impacted the specific performance requirement of Contractor. Contractor is estopped from claiming that a situation has arisen that might otherwise justify changes in the project timetable, the standards of performance under this Contract or the project cost, if Contractor knew of that problem and failed to include it in the applicable report. The deficiency report must be sent to the TXDPS Project Manager ("TXDPS PM").

In the event Contractor identifies a situation wherein TXDPS is impairing Contractor's ability to perform for any reason, Contractor's deficiency report must contain Contractor's suggested solutions to the situation(s). These suggestions should be in sufficient detail so that the TXDPS PM can make a prompt decision as to the best method of dealing with the problem and continuing the project in an unimpeded fashion.

### **34. Substitutions**

Substitutions are not permitted without the written approval of *TXDPS* or *LEA*.

### **35. Vendor Background Checks**

Contractor must have its project personnel submit to a TXDPS fingerprint-based criminal history background investigation, if required by TXDPS. To facilitate this criminal history background investigation, each person must be required to complete a Vendor Background Information form, which will be provided by TXDPS. Contractor is responsible for any costs associated with obtaining any fingerprints for the criminal history background investigation.

If TXDPS requires a fingerprint-based criminal history background investigation, Contractor must not allow personnel to work on the project that have not submitted to and successfully completed a TXDPS fingerprint-based criminal history background investigation.

### **36. Subcontractors**

Contractor must assume full responsibility for all deliverables under the Contract. TXDPS will consider Contractor to be the sole point of Contact with regard to contractual matters, including payment of any and all charges under the contract. If any part of the deliverables are planned to be subcontracted, Contractor must include a list of subcontractors, including the firm name, address, and contact person of each subcontractor, a complete description of the deliverables to be subcontracted, financial statements for each subcontractor, and descriptive information concerning each subcontractor's qualifications.

Contractor must not delegate any duties under the Contract to a subcontractor unless TXDPS has given written consent to the delegation. TXDPS will have the right to approve all subcontractors and to require Contractor to replace any subcontractor found, in the opinion of TXDPS, either initially or based on performance, to be unacceptable. TXDPS reserves the right to receive copies of and review all subcontracts. The management of any subcontractor will be the sole responsibility of Contractor, and failure by a subcontractor to perform will be deemed to be failure of Contractor. Contractor must make all payments to subcontractors and suppliers. TXDPS will not release Contractor from having to perform any obligations under the Contract, notwithstanding the fact that a subcontractor may have been engaged by Contractor to perform those obligations.

All subcontracts shall include all applicable provisions contained in this Contract and any provisions required by law.

### **37. Sales and Use Tax**

TXDPS, as an agency of the State of Texas, qualifies for exemption from state and local sales and use taxes pursuant to the provisions of the Texas Limited Sales, Excise, and Use Tax Act. Contractor may claim exemption from payment of applicable state taxes by complying with such procedures as may be prescribed by the Texas Comptroller of Public Accounts.

### **38. Notices**

Any notice required or permitted under this Contract shall be directed to the respective Parties at the addresses shown below and shall be deemed received: (1) when delivered in hand and a receipt granted; (2) three days after it is deposited in the United States mail by certified mail, return receipt requested; or (3) when received if sent by confirmed facsimile:

If to TXDPS:  
Texas Department of Public Safety

5805 North Lamar Blvd.  
Austin, Texas 78752  
ATTN: Desiree Taylor  
Facsimile: (512) 424-5911

With a copy to:

Texas Department of Public Safety  
5805 North Lamar Blvd., MSC 0130  
Austin, Texas 78752  
ATTN: Chief of Finance, Cheryl MacBride  
Facsimile: (512) 424-2816

If to Contractor:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Either of the Parties may change its address or designated individual(s) to receive notices by giving the other party written notice as provided above, specifying the new address and/or individual and the date upon which it shall become effective.

### **39. Complaints and Contract Claims**

In addition to other remedies contained in this Contract, Contractor may direct their written complaints, as well as any contract claims, to the following office:

Texas Department of Public Safety  
ATTN: Chief of Finance  
5805 North Lamar Blvd., MSC 0130  
Austin, Texas 78752  
Telephone: (512) 424-2062  
Fax: (512) 424-5950  
E-mail: [cheryl.macbride@txdps.state.tx.us](mailto:cheryl.macbride@txdps.state.tx.us)

### **40. Standards for Information Technology**

Contractor must consider and accommodate statewide standards for information technology. These statewide standards are located at <http://www.dir.state.tx.us/standards>.

### **41. Personnel**

Contractor warrants that all persons assigned to the project are employees or subcontractors of Contractor, and are fully qualified to perform the work required herein.

Replacement of personnel, if approved by TXDPS, must be with personnel of equal or greater ability and qualifications. TXDPS will be the arbiter of whether the replacement personnel have equal or greater ability and qualifications than the personnel being replaced.

Contractor must assign all personnel identified in its Offer to complete all of their planned and assigned responsibilities in connection with performance of the obligations of Contractor under this Contract. TXDPS will have the right to approve the assignment and replacement by Contractor of all personnel assigned to provide deliverables or to provide on-site representation of Contractor.

Before assigning a replacement individual for any of the personnel commitments identified in Contractor's Offer, Contractor must notify TXDPS of the proposed assignment, must introduce the individual to the appropriate representatives of TXDPS, must provide a transfer of knowledge validation and must provide to TXDPS a resume and any other information about the individual reasonably requested by TXDPS. TXDPS reserves the right to interview the individual before granting approval.

#### **42. Replacement of Personnel at TXDPS' Request**

TXDPS reserves the right to require Contractor to replace Contractor personnel whom TXDPS judges to be incompetent, careless, unsuitable or otherwise objectionable, or whose continued use is deemed contrary to the best interests of TXDPS or the State of Texas. Before a written request is issued, authorized representatives of TXDPS and Contractor will discuss the circumstances. Upon receipt of a written request from an authorized representative of TXDPS, Contractor must be required to proceed with the replacement. The replacement request must include the desired replacement date and the reason for the request. Contractor must use its best efforts to effect the replacement in a manner that does not degrade deliverable quality. Contractor must also provide TXDPS with evidence of a sufficient transfer of knowledge to the proposed replacement.

This provision will not be deemed to give TXDPS the right to require Contractor to terminate any Contractor employee's employment. Rather, this provision is intended to give TXDPS only the right to require that Contractor discontinue using an employee in the performance of deliverables for TXDPS.

#### **43. Unauthorized Removal of Personnel**

It is critical to the overall success of the project that Contractor not remove or reassign, without TXDPS' prior written approval (which approval will not be unreasonably withheld), any of the assigned personnel until such time as the personnel have completed all of their planned and assigned responsibilities in connection with performance of Contractor's obligations under the Contract. Without prior written approval from TXDPS, personnel will only be changed in the event of death, personal injury or debilitating illness or termination of employment with Contractor. The unauthorized removal of personnel by Contractor will be considered by TXDPS as a material breach of the Contract and grounds for termination.

#### **44. DRUG-FREE WORK PLACE**

The Contractor covenants and agrees that it will comply with the provisions of the Drug Free Work Place Act of 1988 (Public Law 100-690, Title V, Subtitle D; 41 U.S.C. 701 ET SEQ.) and maintain a drug free work; and the final rule government wide requirements

for Drug-Free Workplace (Grants), issued by the Office of Management and Budget and the Department of Defense (32 CFR PART 280, Subpart F) to implement the provisions of the Drug Free workplace Act of 1988 is incorporated by reference and the Contractor covenants and agrees to comply with the provisions thereof, including any amendments to the final rule that may hereafter be issued.

#### **45. Public Safety Commission Approval**

The following TXDPS contracts and commitments must be submitted to the Texas Public Safety Commission or the Commission's designee ("Commission") for review prior to execution, pursuant to Sections 411.003 and 411.004 of the Texas Government Code:

- 1) Any contract or commitment in the amount of \$1,000,000 or more;
- 2) Any change order, individually or in combination with other change orders, that increases the original contract or commitment by fifty percent or more, as long as the dollar amount of the change order(s) is \$100,00 or more; or
- 3) Any change order, individually or in combination with other change orders, that increases the original contract or commitment by \$500,000 or more.

#### **46. Interpretation Against the Drafter**

Regardless of which party drafted the Contract or the language at issue, any ambiguities in the Contract or the language at issue will not be interpreted against the drafting party.

#### **47. Non-incorporation Clause**

This contract embodies the entire agreement between the Parties regarding the project described in this Contract, and there have been and are no oral or written covenants, agreements, understandings, representations, warranties or restrictions between the Parties regarding the project described in this Contract other than those specifically set forth herein.

#### **48. Multiple Contracts**

This Contract may be executed in a number of identical counterparts, each of which shall be deemed an original for all purposes. In making proof of this Contract, it shall not be necessary to produce or account for more than one such counterpart.

#### **49. Headings**

The headings, captions and arrangements used in this Contract are, unless specified otherwise, for convenience only and shall not be deemed to limit, amplify or modify the terms of this Contract, nor to affect the meaning thereof.

#### **50. Licenses and Permits**

This section entitled "Licenses and Permits" only applies to intellectual property which is not developed under this Contract and to which TXDPS does not already have a right to use, display and reproduce.

Contractor is not authorized to include such intellectual property in any deliverables, unless Contractor receives the written authorization from TXDPS project manager to do so.

### **50.1 Third Party Intellectual Property**

Vendor shall pay all license fees and/or royalties and assume all costs incident to the use or possession in the performance of the deliverables or the incorporation into the deliverables of any third party intellectual property.

If Vendor incorporates any proprietary third party intellectual property into the deliverables, Vendor shall obtain and furnish with such intellectual property the following: (i) documentation on the use of such intellectual property, (ii) a perpetual, irrevocable license (which may be nontransferable, nonexclusive, or both) to reproduce, publish, display and otherwise use, or modify such intellectual property and associated user documentation, and (iii) a perpetual, irrevocable license (which may be nontransferable, nonexclusive, or both) to authorize others to reproduce, publish, display and otherwise use, or modify such intellectual property for TXDPS purposes. Vendor will facilitate the transfer of third party licenses to TXDPS upon terms and conditions acceptable to TXDPS. For those third party products that require license renewal, TXDPS has the option to arrange licensing directly from the suppliers.

### **50.2 Vendor's Intellectual Property**

This Contract shall supersede all terms of any "shrink-wrap" or "click wrap" license included in any package, media or electronic version of the intellectual property and any such intellectual property shall be licensed or provided under the terms of this Contract.

In consideration of payment in full of the applicable purchase price for the applicable deliverable, Vendor hereby grants to TXDPS a perpetual, irrevocable, paid-up, nonexclusive and enterprise-wide license to allow TXDPS and the TXDPS designees to use, display, publish, reproduce and modify the intellectual property. Vendor reserves all rights to the intellectual property that have not been expressly granted to TXDPS.

TXDPS has the right, in its own discretion, to independently modify and create derivative works of such intellectual property to which a license is granted to TXDPS herein, through the services of TXDPS' own employees or any independent contractors. TXDPS shall own all rights to such modifications or derivative works.

## **51. Warranties**

### **51.1 Third Party Warranties**

If, under this Contract, the Contractor procures any materials or products for TXDPS, the Contractor must assign or otherwise transfer to TXDPS, or afford TXDPS the benefits of, any manufacturer's warranty for such materials or products.

### **51.2 Contractor Warranties**

Contractor warrants that all deliverables will be free from defect in materials and workmanship, and that all deliverables will comply with the TXDPS specifications, for a period of one (1) year. The warranty period will begin upon acceptance by TXDPS of each deliverable provided in accordance with the provisions of this Contract. If software is included as a deliverable under this Contract, all software releases and upgrades released during the warranty period must be provided to TXDPS at no cost.

The Contractor/subcontractor(s) make the following representations and warranties, including without limitation, the following:

The Contractor/subcontractor(s) must create and deliver all deliverables in accordance with the highest professional standards in the industry.

The Contractor/subcontractor(s) must use adequate numbers of qualified individuals with suitable training, education, experience, and skill to create and deliver the deliverables.

The Contractor/subcontractor(s) must maintain all equipment and software for which it has maintenance responsibilities in good operating condition and must undertake all repairs and preventive maintenance in accordance with the manufacturers' recommendations.

The Contractor/subcontractor(s) must use its best efforts to use efficiently all resources or services necessary to provide the deliverables that are required under this Contract.

The Contractor/subcontractor(s) must use its best efforts to create and deliver the deliverables in the most cost-effective manner consistent with the required level of quality and performance.

The Contractor/subcontractor(s) must create and deliver the deliverables in a manner that does not infringe the proprietary rights of any third party.

The Contractor/subcontractor(s) must create and deliver the deliverables in a manner that complies with all applicable laws and regulations.

The Contractor has duly authorized the execution, delivery, and performance of this contract.

The Contractor/subcontractor(s) has not provided any gifts, payments, or other inducements to any officer, employee or agent of TXDPS.

The Contractor/subcontractor(s) must use its best efforts to ensure that no viruses or similar items are coded or introduced into any systems used to create or to deliver the deliverables.

The Contractor/subcontractor(s) must not insert or activate any disabling code into any systems used to create or to deliver the deliverables without TXDPS express prior written approval.

The Contractor/subcontractor(s) will not infringe any intellectual property right of any third party. In the course of performing work under this Contract, Contractor/subcontractor(s) will not use or copy any intellectual property owned by a third party without paying any required license fees or royalties.

The Contractor/subcontractor(s) will not use or incorporate any open source software into any of the deliverables under this Contract without the written approval from the TXDPS PM.

## **52. Liquidated Damages**

TXDPS reserves the right to assess liquidated damages at an amount equal to \$400.50 per-day for each calendar day beyond the expected date of Final Operating Capability for each deliverable. The Parties acknowledge that the harm that will be caused to TXDPS by such a delay is difficult to estimate; however, the amount of liquidated damages listed herein is a reasonable estimate and is enforceable. Contractor shall not be responsible and liquidated damages may not be assessed due to any delay caused by schedule amendments requested by TXDPS, delays as the result of activity that is the responsibility of the TXDPS project team as long as Contractor timely files its deficiency report as required by the Section herein entitled "Rolling Estoppel" or delays that TXDPS deems were outside the control of the Contractor. Assessments incurred under this provision may, at TXDPS' option, be deducted from any payment due the Contractor. The burden of proof that the delay is attributable to TXDPS rests with Contractor. TXDPS has the right to offset any liquidated damages payable to TXDPS, as specified above, against any payments due to Contractor. If insufficient payments are available to offset such liquidated damages, then Contractor shall pay to TXDPS any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

## **III. ACCEPTANCE OF DELIVERABLES AND PROJECT UPDATES**

### **1 Schedule**

Contractor must provide the TXDPS PM or LEA PM with a deliverable schedule that includes date expectations for completion of each deliverable provided, along with the itemized cost for each deliverable. Schedule must include any TXDPS or LEA responsibilities or expectations that could adversely affect the completion of any deliverable. TXDPS PM or LEA PM must approve the schedule prior to Contractor beginning any billable work. Work performed before approval of the schedule will be at vendor's risk and will not be reimbursed.

### **2 Statement of Work**

Contractor must prepare and deliver a Statement of Work ("SOW"), to the TXDPS PM or LEA PM in response to a request for RRMS Enhancements or Modifications for each deliverable as describe in the RRMS RFO.

### **3 Inspections and Tests**

All aspects of this Contract will be subject to inspection and test by TXDPS or LEA. Tests will be performed on each documented deliverable if applicable and will require joint signoff by Vendor and TXDPS or LEA personnel. The testing will verify successful implementation of each deliverable. The test schedule and test plan will be developed jointly by the TXDPS or LEA and the Contractor.

All costs shall be borne by the Contractor in the event any deliverable tested fails to meet or exceed all conditions and requirements of the specifications. Latent defects may result in revocation of acceptance. A written acceptance form that describes the

deliverable, the previously agreed-to acceptance criteria, with space for sign-off by both the TXDPS PM or LEA PM and Contractor will be provided.

If a deliverable provided is rejected, the reasons for rejection must be documented. TXDPS or LEA may only be able to tell the Contractor that the deliverable provided does not work. TXDPS or LEA is relying on the expertise of the Contractor to develop a compliant deliverable and to fix noncompliant deliverables. The lack of a signature on the acceptance form does not constitute rejection and cannot be used by the Contractor as a default acceptance. The TXDPS PM or LEA PM will maintain all signed acceptance forms.

#### **4 Project Status Updates**

TXDPS or LEA will require the Contractor provide, on a weekly basis or other mutually agreed upon schedule, a project status update. It will be at the sole discretion of TXDPS or LEA to approve the method of weekly status updates. The Contractor must keep TXDPS or LEA advised at all times of the status of the project. All delays whether foreseen or unforeseen in delivery or implementation must be provided to the TXDPS PM or LEA PM in writing within five (5) business days of determination of delay. Contractor must include the following in its delay documentation: a) a date, b) the reason for delay, c) the Party who is at fault regarding the delay and d) a reasonable expectation for resolution. Default in promised delivery (without accepted reasons) or failure to meet specifications, authorizes TXDPS or LEA to purchase deliverables elsewhere and charge full increase in costs, if any, to the Contractor, in addition to any other legal or equitable remedy.

#### **5 Final Operating Capability**

Final Operating Capability is defined as the successful completion and final acceptance by TXDPS or LEA of any deliverable. TXDPS or LEA expects that every deliverable will meet expectations outlined in the RFO and the agreed upon SOWs for this RFO. After each deliverable provided complies with the requirements of Final Operating Capability, the Contractor may submit an invoice for such. Vendor will be responsible for providing TXDPS PM with a Project Completion Acceptance Form for acceptance by signature.

#### **6 Product Upgrades**

Product upgrades or new version releases for RMS Software and services, JMS Software and services or CAD Software and services must be installed or placed into service at a time agreeable to both TXDPS (and/or the LEA) and the Contractor including any necessary training, documentation or manual updates; however, the installation, implementation, training and document updates must occur no later than 60 calendar days immediately following the first day the software or service is available for purchase. Product upgrades and new version releases are required to maintain prior software(s) or service(s) interface functionality including but not limited to: data extraction, data export, data import.

### **IV. SERVICE LEVELS FOR WARRANTY**

Warranty work shall be performed solely by Contractor. Due to the nature of the system, all hardware (as applicable to this contract), hardware installations (as applicable to this contract), software, software enhancements and programming services warranty work must follow requirements provided in the RFO. Vendor must resolve System down time within two (2) hours of first report for those within its control. Contractor must provide 24/7 toll-free help desk for reporting issues. Contractor must resolve all other issues within twenty-four (24) hours of report for issues not deemed critical in nature by the TXDPS PM or the LEA PM.

IN WITNESS WHEREOF, the Parties to this Contract have signed and delivered this Contract.

\_\_\_\_\_  
(Company name)

By: \_\_\_\_\_

Date: \_\_\_\_\_

**Texas Department of Public Safety:**

By: \_\_\_\_\_

Date: \_\_\_\_\_

**APPENDIX K**

**TXDPS RRMS SERVICE LEVEL AGREEMENT  
USER SUPPORT**

# **REMOTE CRIMINAL RECORDS SYSTEM MANAGEMENT (RRMS) SERVICE LEVEL AGREEMENT**

The purpose of this Service Level Agreement (SLA) is to ensure that the proper elements are in place to provide RRMS stakeholders with optimal level of system performance. This SLA defines the terms, conditions, requirements, responsibilities and obligations of the Texas Department of Public Safety (TXDPS), local law enforcement agencies and users as well as the Vendor.

This SLA has been made by and between \_\_\_\_\_  
(hereinafter referred to as "Vendor") with a place of business at \_\_\_\_\_ and the  
Texas Department of Public Safety with a place of business at 5805 Lamar, Austin, TX  
78752 hereinafter referred to as "TXDPS").

## **1. Definitions**

Where any word or phrase defined below, or a pronoun used in place thereof is used in any part of this SLA, it shall have the meaning herein set forth.

### **APPLICATION SOFTWARE**

A computer program which is intended to be executed on the RRMS purchased from the VENDOR.

### **COMMUNICATION**

The process employed for information transmission or telecommunication including such elements as routers, switches, internet service providers (ISP), protocols, virtual private network (VPN), etc. used in the .

### **CONTRACT**

Set of documents as defined in the RRMS CONTRACT Section II(1) TERMS AND CONDITIONS.

### **CUSTOMER**

Authorized local and state law enforcement agencies are the primary RRMS CUSTOMERS.

### **DOCUMENTATION**

All material to be delivered by the VENDOR either in hard copy format or made available through the RRMS. This includes but is not limited to DOCUMENTATION listed in the RRMS RFO Section 8.9.2 DOCUMENTATION.

### **DOWNTIME**

The period of time when the RRMS is NOT available (including outages, unscheduled events for remedial maintenance, Failures, etc) to the CUSTOMERS or USERS.

## FAILURE

Undesirable SYSTEM PERFORMANCE resulting in DOWNTIME.

## FAILURE RATE

The frequency of time when the RRMS is NOT available to the CUSTOMERS or USERS

## HARDWARE

The physical components used in the SYSTEM PERFORMANCE of the RRMS.

## HOSTING SERVICES

Computer-based services utilized in making available the RRMS to authorized CUSTOMERS and USERS.

## INDEX SEARCH

A search initiated by the RRMS USER using unique fields such as SSN, DL, SID, TYC, FBI, TDCJ, Case no., etc.

## INTERNET SERVICE PROVIDER (ISP)

The CUSTOMER'S or USER'S company which provides access to the Internet (also known as Internet Access Providers).

## OPERATIONAL USE TIME

The time during which the RRMS is in actual operation and serving the intended CUSTOMERS and USERS at optimal level of performance.

## POWER UPTIME

Period of time when the RRMS is available to CUSTOMERS and USERS for any purposes excluding training and testing.

## PREVENTIVE MAINTENANCE

Any task not considered remedial and is routinely performed as part of a regularly scheduled program of Maintenance, designed to keep the RRMS in proper operating condition. The primary goal of maintenance is to avoid or mitigate the consequences of failure of the RRMS.

## PRINCIPAL PERIOD OF MAINTENANCE

The PRINCIPAL PERIOD OF MAINTENANCE COVERAGE is Monday through Friday during the hours of 8:00 a.m. to 5:00 p.m. excluding state or federal holidays.

## RECORDS

All data, images, or information owned and contributed by the CUSTOMER and stored by the RRMS.

## REMEDIAL MAINTENANCE

Maintenance performed by the VENDOR which results from RRMS FAILURE and which is performed on an unscheduled basis.

#### RESPONSE TIME

The quantity of time in which the RRMS takes to react and return a response to a USER'S ISP. RESPONSE TIME is the interval between the instant at which the USER at a workstation enters a request for a response and the instant at which the first character of the response is received by the CUSTOMER/USER'S ISP. RESPONSE TIME is must be real time or near real time.

#### RRMS

The entire collection of real or abstract information technology which execute the SYSTEM PERFORMANCE requirements of this CONTRACT **excluding** CUSTOMER'S or USER'S HARDWARE, SOFTWARE, or access methodology.

#### SOFTWARE

The computer programs or collection of computer programs, middleware, applications, procedures, environments, Operating Systems, utilities, platforms, tools, drivers, interfaces, web services, graphical user interface (GUI), etc. used in the SYSTEM PERFORMANCE of the RRMS.

#### SOFTWARE ENGINEER

VENDOR personnel with in-depth expertise who provide technical support in each area of SOFTWARE functionality, including the Operating System, and all application SOFTWARE.

#### SOFTWARE VERSION RELEASES

Modifications to the SOFTWARE which resulted from extensive changes, substantial revision or version upgrade; thoroughly tested, debugged and ready for production or live release.

#### SPECIAL MAINTENANCE

Services performed by the VENDOR outside the scope of specified PREVENTIVE MAINTENANCE, REMEDIAL MAINTENANCE, OR SOFTWARE Support services.

#### SYSTEM PERFORMANCE

The process of effectively fulfilling the intended purpose or tasks.

#### USER

CUSTOMER'S authorized staff that access or use the RRMS.

#### VENDOR

TXDPS RRMS Certified Provider

## **2. Maintenance**

Maintenance regarding CUSTOMER'S or USER'S HARDWARE, CUSTOMER'S or USER'S SOFTWARE, CUSTOMER'S or USER'S Network or CUSTOMER'S or USER'S access methodology is the responsibility of the CUSTOMER and is outside the scope of this Contract. VENDOR must provide notice to CUSTOMER'S and USER'S at a minimum of three (3) business days prior to scheduled maintenance including length of anticipated DOWNTIME plus the description or purpose of scheduled maintenance. VENDOR must provide notice to CUSTOMERS and USERS prior to un-scheduled Maintenance where possible including length of anticipated DOWNTIME plus the description or purpose of un-scheduled maintenance.

## **2.1 Preventive Maintenance**

VENDOR agrees to provide preventive maintenance services in order to maintain the RRMS in good condition and working order on a mutually agreeable scheduled basis. The preventive maintenance schedule is to be based on VENDOR'S and CUSTOMER'S mutual agreement of the particular service required for each system component, it being understood that this schedule shall be oriented around periods when the system is expected to have the lightest use and outside of the PRINCIPAL PERIOD OF MAINTENANCE.

## **2.2 Remedial Maintenance**

VENDOR agrees to provide REMEDIAL MAINTENANCE to the RRMS on a twenty-four (24) hour per day, seven (7) day per week basis, with a response time of no more than two (2) hours each incident.

**2.2.1.** During the term of this AGREEMENT, CUSTOMER may, by providing thirty (30) days prior written notice, select any alternative period of maintenance coverage as a modification to this AGREEMENT whether or not such alternative represents an increase or decrease in service.

## **2.3. Special Maintenance Services**

The following maintenance services are outside the scope of PREVENTIVE MAINTENANCE and REMEDIAL MAINTENANCE as described above and shall be considered SPECIAL MAINTENANCE service items:

- Repair of defects in the system resulting from causes beyond the control of CUSTOMER and/or VENDOR, such as acts of God;
- Repair of defects in the HARDWARE, SOFTWARE, Network, or any other component of the RRMS.

VENDOR agrees to perform SPECIAL MAINTENANCE during periods when the system is expected to have the lightest use and outside of the PRINCIPAL PERIOD OF MAINTENANCE whenever possible.

## **3. *RRMS Production Control***

VENDOR must schedule production management such as batch processing, job scheduling, automated import/exports, etc at a minimum of once every twenty-four (24) hours, seven (7) days per week and three hundred sixty-five (365) days per year. The production control schedule must be mutually agreed upon by both the VENDOR and CUSTOMER and must be oriented around periods when the system is expected to have the lightest use.

#### **4. RRMS Hardware**

Title to all RRMS HARDWARE and parts provided by the VENDOR shall remain with the VENDOR. Parts replaced and removed from the RRMS HARDWARE provided by the VENDOR are the property of VENDOR. All CUSTOMER data and/or images resident on replaced HARDWARE or parts MUST be permanently erased, removed, reformatted or deleted from all HARDWARE or parts removed by the VENDOR.

#### **5. RRMS Support**

VENDOR shall support all RRMS SOFTWARE licensed to CUSTOMERS for use during the term of the RRMS CONTRACT. VENDOR agrees to provide CUSTOMER support for the RRMS Monday through Friday 7:00 a.m. (C.D.T/C.S.T) to 6:00 p.m. (C.D.T/C.S.T) excluding state or federal holidays, through a VENDOR provided toll-free telephone, facsimile, or e-mail. VENDOR must provide the capability for the CUSTOMERS and USERS to leave a message for occasions outside of that time period. VENDOR must identify a problem escalation plan which must be included in the DOCUMENTATION.

VENDOR must staff the CUSTOMER Support telephone center with adequate number of personnel to meet the service level goal of answering 90% of the calls within three (3) minutes. VENDOR agrees to maintain sufficient representatives on their CUSTOMER service call center staff who are fluent in Spanish.

RRMS Support consists of identifying, verifying, reporting, and resolving problems associated with RRMS SOFTWARE licensed to CUSTOMER in order to maintain optimal RRMS SYSTEM PERFORMANCE at a level equal to the requirements.

- 5.1. RRMS CUSTOMER and USER Support **includes** responsibilities such as:
- RRMS Product sales
  - New CUSTOMER training (new procurements only)
  - RRMS configuration
  - RECORD contribution methodologies or practices
  - RRMS navigation
  - Data query or export procedures
  - Search criteria, best practices, parameters, etc.
  - Troubleshooting for RRMS HARDWARE, SOFTWARE, Network, etc.

4.2. RRMS CUSTOMER and USER Support **excludes** responsibilities such as:

- RECORD content
- RECORD quality
- RECORD interpretation
- USER administration (including new accounts, password creation or resets)
- Non-RRMS SOFTWARE owned, purchased, installed, developed or utilized by the CUSTOMER or the CUSTOMER'S HARDWARE
- CUSTOMER/USER'S ISP or other internal method of access

## **6. Software Updates**

VENDOR shall provide periodic RRMS SOFTWARE updates that shall incorporate (i) corrections of any defects, and (ii) at the sole discretion of VENDOR, enhancements to the RRMS SOFTWARE.

6.1. RRMS SOFTWARE updates released by VENDOR shall be installed by VENDOR during periods when the RRMS is expected to have the lightest use and outside of the PRINCIPAL PERIOD OF MAINTENANCE at no charge to CUSTOMER.

6.2. Updates to DOCUMENTATION or manuals resulting from RRMS SOFTWARE updates shall be provided or made available on demand to CUSTOMERS and USERS free of charge.

## **7. RRMS System Performance**

### **7.1. Basic Requirements**

VENDOR agrees to maintain optimal RRMS SYSTEM PERFORMANCE twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year at a rate of 99.5% (hereafter referred to as the "RATE") as calculated by SLA Section 6.2 Rate Calculation. VENDORS are cautioned to quickly resolve the source or sources of Failure. Inability to meet or exceed the RATE in any eighteen (18) month period will result the following actions:

- First event – verbal warning
- Second event – written warning added to the Contract file
- Third event – Contract termination and Vendor Performance reported as "Poor"

### **7.2. Rate Calculation**

VENDORS will measure the RATE of SYSTEM PERFORMANCE for the RRMS by the amount of DOWNTIME during a calendar month. This metric gauges the SYSTEM PERFORMANCE as a percentage of available hours tracked to the quarter of an hour (rounded). The RATE of SYSTEM PERFORMANCE will be measured and monitored for the RRMS as follows:

- 7.2.1. Available hours equal total number of hours in a month (24 hours x number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled maintenance for the hosted application.
- 7.2.2. DOWNTIME is the total number of hours (to the quarter hour-rounded) during which the RRMS is not in OPERATIONAL USE TIME.
- 7.2.3. SYSTEM PERFORMANCE RATE equals available hours minus DOWNTIME divided by available hours.

EXAMPLE FOR THE MONTH OF JANUARY:

Available time per month was 744 hours (31 days X 24 hours)

DOWNTIME per month was 3.75 hours (start 1:00 am - end 4:40 am)

$$744.00 - 3.75 = 740.25$$

$$740.25 \div 744 = 99.5\%$$

### **7.3. Response Time**

Vendors will maintain a real-time or near real-time RESPONSE TIME for INDEX SEARCHES not to exceed a maximum of twelve (12) seconds per INDEX SEARCH. RESPONSE TIME will be reported as the average of the total RESPONSE TIME for the total quantity of INDEX SEARCHES submitted by CUSTOMERS and USERS. Time period used in calculating the RATE will be used to calculate the RESPONSE TIME average.

EXAMPLE FOR THE MONTH OF JANUARY:

Total INDEX SEARCHES = 510

Total RESPONSE TIME = 6,108 seconds

$$6,108 \div 510 = 11.98 \text{ seconds}$$

### **7.4. Reports**

VENDOR will report both SYSTEM PERFORMANCE RATE and average RESPONSE TIME of the RRMS no later than the tenth (10<sup>th</sup>) calendar day of each month to TXDPS and all local CUSTOMERS for the previous month. Reports may be made available through the RRMS or distributed to CUSTOMERS Contact.

### **8. Data Backups**

VENDOR must perform backups on all RRMS RECORDS once every twenty-four (24) hours, seven (7) days per week and three hundred sixty-five (365) days per year to facilitate data and RRMS System restoration in the event of any FAILURES, including but not limited to HARDWARE. The data backup schedule must be mutually agreed upon by both the Vendor and CUSTOMER and must be oriented around periods when the RRMS is expected to have the lightest use.

### **9. Contact Persons**

VENDOR shall designate a person or persons as the primary point of contact for the CUSTOMER. The CUSTOMER shall designate a person or persons as the primary

point of contact for the VENDOR. VENDOR must identify detailed contact information in the event of an outage or an emergency plus an escalation plan.

## APPENDIX L

### **Law Enforcement Information Technology Standards Council (LEITSC) Standard Functional Specifications for Law Enforcement Computer Aided Dispatch**

Offer Package # 3, posted separately to the ESB