**STATE OF TEXAS** § 
§ 
**COUNTY OF TRAVIS** §

### OFFENDER MONITORING AND TRACKING SYSTEM (ELECTRONIC BED CHECK) INDEFINITE DELIVERY INDEFINITE QUANTITY (IDIQ)

### CONTRACT NUMBER CON0001079

This contract is effective **August 27, 2019**, and is by and between the **Texas Juvenile Justice Department**, hereinafter **TJJD**, and the **Cooper Consulting, Company, 1705 Crossing Place, 101A, Austin, Texas 78741**, hereinafter **Service Provider**, to develop/configure, test, stage, and release an Offender Monitoring and Tracking System (OMTS).

This Agreement is composed of the following documents:

1.  This contract, including all exhibits/attachments;
2.  Request for Proposal (RFO) #644-9-070319, and all RFO addendums, hereby incorporated by reference;
3.  Service Provider's proposal dated August 2, 2019, as modified by Service Provider's Best and Final Offer (BAFO) emails dated August 15, 2019, August 16, 2019, August 19, 2019, and August 23, 2019, and Clarification emails dated August 7, 2019, August 9, 2019, and August 12, 2019, all hereby incorporated by reference; and
4.  Service Provider's DIR Contract # DIR-TSO-3904, hereby incorporated by reference.

In the event there is conflict between the Agreement documents, the order of precedence shall be the order listed above, unless otherwise indicated.

### SECTION I: CONTRACT TERM

The contract will be for an Indefinite Delivery Indefinite Quantity (IDIQ) deployment of the OMTS. There will be a minimum purchase, initial Assignment, to address the requirements of the contract. Subsequent Assignments, purchases of services and/or equipment, if any, will be as needed and are not guaranteed, but will be effectuated through contract amendment, if applicable. The IDIQ contract will consist of an initial term of approximately two (2) years as a base period from **August 27, 2019, through August 31, 2021,** with four (4) additional one (1) year option periods beginning on September 1, 2021 - August 31, 2022, September 1, 2022 - August 31, 2023, September 1, 2023 - August 31, 2024, and September 1, 2024 – August 31, 2025. Renewals will be agreed upon by both parties in writing by contract amendment. Any renewals shall be at the same terms and conditions stated in the contract, including any approved changes.

**SECTION II: SERVICE PROVIDER**

## 1   SCOPE

Service Provider will develop/configure, test, stage, and release a Youth Offender Monitoring and Tracking System (OMTS)  solution that provides the ability to track youth throughout the facility. The Service Provider will work in a team-based Agile environment. TJJD's Information and Communication Technology (ICT) team will work with the Service Provider to create and maintain system roadmaps, project plans, and product and release backlogs that will be the basis for the Service Provider's work. TJJD will also provide a Product Owner who will further specify high-level requirements to the Agile team. As in typical Agile processes, TJJD Product Owner will work together with the team to develop and estimate user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. TJJD Product Owner, supported by subject matter experts(SMEs) and business analysts, will determine whether acceptance criteria have been satisfied.

### 1.1   General System Capabilities

Service Provider's OMTS solution, at minimum shall:

1.1.1   Track Youth Offenders throughout the facility.

1.1.2   Track Youth Offender movement history from the front-end and back-end of the application. This means the historical orders/appointment must detail where the Youth Offender was at that point in time (facility and housing area).

1.1.3   Schedule appointments to a combination of facility/service types in order to populate service queues at the time of the appointment. Appointments must follow Youth Offender to new facility and service type automatically, even when initially ordered at a different facility/provider.

1.1.4   Capture well-being checks and observations of youth.

1.1.5   Provide centralized management and administration component to track safety checks and access at a centralized as well as site level in real-time.

1.1.6   Integrate the OMTS with a case management system via API.

1.1.7   Provide tools for user to customize forms, create templates, and smartforms to capture data relevant to monitoring and tracking youth offender.

1.1.8   Provide alerts: Ability to set alerts based on any field, general area of the Youth Offender record, or at points in time; ability to create alerts based on multiple criteria; and pop ups and other mechanisms to alert users, guide workflow to ensure monitoring occurs

systematically and periodically throughout the day.

1.1.9 Provide Decision Support tool inclusive of specific housing placement, and correctional/customized fields to facilitate monitoring according to Youth Offender classifications.

1.1.10 Provide reporting capabilities to track Youth Offenders, the status of their well-being, and their location.

1.1.11 Place Youth Offenders on a queue even if the Youth Offender is discharged. Must also be able to document on a discharged person's record.

1.1.12 Provide the Suicide watch functionality to allow for additional monitoring of specified youth.

**1.2**  **Locations**

Service Provider shall deliver services to each of the secured and halfway house facilities identified below:

1.  **Evins Regional Juvenile Center**
    3801 E. Monte Cristo Road
    Edinburg, Texas 78541
    Pods: 10

2.  **Gainesville State School**
    1379 FM 678
    Gainesville, Texas 76240
    Pods: 12

3.  **Giddings State School**
    2261 James Turman Road
    P.O. Box 600
    Giddings, Texas 78942
    Pods: 16

4.  **McLennan County State**
    Juvenile Correctional Facility
    116 Burleson Road
    Mart, Texas 76664
    Pods: 22

5.  **Ron Jackson State Juvenile**
    **Correctional Complex**
    611 FM 3254

Brownwood, Texas 76801
Pods: 14

6. **Ayers House**
   17259 Nacogdoches Road
   San Antonio, Texas 78266
   Pods: 1

7. **Brownwood Halfway House**
   910 FM 3254
   Brownwood, TX 76801
   Pods: 1

8. **Edna Tamayo House**
   1438 N. 77th Sunshine Strip
   Harlingen, Texas 78550
   Pods: 1

9. **McFadden Ranch**
   3505 N. Haynes Road
   Roanoke, Texas 76262
   Pods: 2

10. **Schaeffer House**
    12451 Garment Road
    El Paso, Texas 79938
    Pods: 1

11. **Willoughby House**
    8100 W. Elizabeth Lane
    Fort Worth, Texas 76116
    Pods: 1

The Service Provider may deliver services to additional locations as identified by TJJD.

### 1.3    Component Devices Requirements

Service Provider's OMTS devices, at minimum, must:

1.3.1    Be able to provide digital/ tagging of housing locations across each of the sites listed in Section 3.2.

1.3.2    Provide the ability for staff to log in/log out for their assigned account.

1.3.3    Be scalable and interoperable with other component technologies (please specify in your

response). Scalability and interoperability standard compatibility.

1.3.4 Include the number of devices requested by TJJD, docking unit for each device, and two swappable batteries for each device to equip correctional officers to track youth offenders in real-time.

## 1.4 Electronic Bed Check Requirements

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.4.1 Security Check - electronically logs staff physical presence at each significant step of their security round.

1.4.2 Room Check - captures face-to-face interactions, observations, and behaviors of juveniles at frequent intervals (e.g. every 15 minutes).

1.4.3 Out of Room - digitally records all movements.

1.4.4 Meals & Recreation digitally logs all meals provide in living units and recreation or exercise events.

1.4.5 Medication – digitally logs all medication provided to youth in living units

1.4.6 Headcount - confirms number of juveniles per living unit and various group events for security and accountability.

## 1.5 Business Rules Validation Requirements

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.5.1 Ability to force users to answer any questions or ability to have hard stop preventing user from locking a record if they have not completed certain requirements.

1.5.2 Data Validation - ability to restrict bad data entry i.e. not allow text in date fields, not allow numbers, etc.

1.5.3 Ability to lock down fields so that users cannot change the text or descriptions.

1.5.4 Ability to create user roles and permissions based on varying criteria.

## 1.6 Security Logs Requirements

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.6.1　Ability to record history of every action taken on a Youth Offender record by users viewing or modifying the record; Ability to easily obtain those records for reporting purposes.

1.6.2　Ability to classify housing areas.

1.6.3　User Logs - ability to record history of every action taken by a user.

1.6.4　Ability to designate Youth Offender and parts of entire record that can be reviewed by external parties.

1.6.5　External party can only see designated Youth Offenders.

1.6.6　Youth Offenders sometimes refuse services. Refusals must still be documented on scheduled appointments for stipulation purposes.

1.6.7　Configure offenders, officers, assets, locations, and observations.

1.6.8　Ability to create groups, well-being check rules, and location inspection rules.

1.6.9　Send notifications and alerts to desired personnel when rules are broken.

1.6.10　Ability to configure Agency defined alerts.

1.6.11　Ability to specify rules and restrictions depending on the offender and location.

1.6.12　Expandable for multiple locations.

**1.7　Health Services Monitoring Requirements**

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.7.1　Some Youth Offender medications will need to automatically indicate a change from carry to non-carry depending on Youth Offender specific, facility, and/or housing area update.

1.7.2　Youth Offender information must be visible alongside clinical details by each service type/housing area combinations to allow for rapid clinical response in the correctional environment.

1.7.3　Ability to prioritize Youth Offenders on service queues based on medical condition or other criteria.

1.7.4　Provide a service queue for nursing services:

- Examples include: Diabetic care, wound care, Clinical Institute Withdrawal Assessment CIWA, Librium.

- Nursing care modules to drive care: Infirmary level – assessments, treatment plans, goals.

1.7.5   Bed management – tracking Youth Offender, orders, and drugs, approved medical devices; ability to produce daily reports to Direct Care Staff per Youth Offender of approved devices tracking specialty appointments and services by Youth Offender/bed.

1.7.6   Ability to designate units within infirmary for different Youth Offender security classification.

1.7.7   Ability to provide an accurate list of a Youth Offender's current medications.

1.7.8   Rx Classification - Formulary/Non-formulary/Restricted

1.7.9   Some housing areas are carry and others non-carry. Built in logic to match medication restrictions to housing area.

1.7.10  Clinical administrative user permission to create customizable medication schedule at facility level.

1.7.11  Ability to allow users to set up instructions so that providers can see instruction while ordering meds.

1.7.12  Ability to build tapers– e.g. for methadone, prednisone, etc.

1.7.13  Ability to order tapers.

1.7.14  Ability to easily correct medication orders prescribed by mistake e.g. not have to schedule new appointment or create new encounter.

## 1.8   Business Intelligence Requirements

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.8.1   Ability to equip supervisors with real-time and historical insights about daily floor operations, juveniles, and staff members.

1.8.2   Ability to measure round compliance in real-time with customizable warnings, notifications, and digital clocks help to communicate security round performance.

1.8.3   Ability to gathers floor activities from across the facility and centralizes them into one single information feed.

1.8.4   Ability to generate electronic reports that can be filtered by juvenile name, activity type,

and more.

1.8.5   Ability to present visualized Dashboards that establishes a body of evidence for each formal count, while visualizing scans in real-time.

1.8.6   Ability to locate juveniles during scheduled activities, and flags juveniles with returnable supplies.

## 1.9   Technical Requirements

### 1.9.1   Security

TJJD must be able to safeguard certain confidential information and control who can do what to the various information. Audit trails must be available to allow the reconstruction of data change, access, and search activities. Individual security rights should be able to be controlled at the user level and should be consistent to all access to information.

Service Provider should provide software and database security features. In particular, TJJD requires user-defined privileges, authentication, network, and database security modules; information sharing security (e.g., encryption, user-defined privileges, medical and other legal considerations, FERPA, HIPAA, FBI-CJIS, auditing concerns, mechanisms for tracking access and updates, interface interactions). Service Provider must specify and provide solution that addresses security concerns. In addition, solutions that incorporate technical privacy, and enable redacting of erroneous information through data dumps, etc. (user-defined privileges, data filters when sharing information) and consideration of local privacy laws.

1.9.1.1   The application should be compliant with the State of Texas' TAC 202 requirements and be guarded against known and new vulnerabilities such as:

- SQL Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Un-validated Redirects and Forwards
- Service Provider's system must be accessible from different domains on the Agency network.
- Domain trust relationships shall be avoided when another communication method is available.
- Domain trust relationships between systems shall be introduced according to business requirements and must be documented.

- If hardware requirements are required on-premises, the Service Provider must provide ports, services, and applications not servicing business requirements must be disabled.
- Service Provider must also address any vulnerabilities identified as risk assessment.
- User sessions shall automatically log off after a set period of inactivity. The set period shall be customized to the level of user access, and the period may be modified by a system administrator.

### 1.9.2 Audits and Controls Requirements

This section addresses both the requirements for "internal" and "external" auditing capabilities. The system shall have controls to ensure data integrity. Audit trails must be available to assist in identifying basic information such as: What was changed? Who changed it? When was it changed?

### 1.9.3 User Management and Security Requirements

Service Provider's OMTS solution, at minimum shall, at a minimum, provide the following capabilities:

1.9.3.1 User Levels - The system shall allow for at least 700 users with varying levels of security privilege that determine which parts of the system are accessible and editable.

1.9.3.2 Archiving - The system shall retain all non-active staff user records in the system and all records shall retain these users as connected and owners of the journals, events and other components created or recorded while that TJJD staff person was at TJJD.

1.9.3.3 Outgoing Staff transfers - The system cases and any activities outstanding shall be transferred in bulk or individually to new supervising case managers, probation or parole officers in the event of a TJJD staff person terminating their employment or being transferred out of active supervision.

1.9.3.4 Security Requirements

    a. The system must provide for role based access to information that takes into consideration
        i. Role of the user
        ii. The type of data being accessed

    b. User Roles - Access to data, reports, and system setup will be based on user roles. Access levels include: No Access, View, Create, Maintain, and Delete.

    c. Super User - The system must provide for the use of a super user role with the ability to review all aspects of the system. This role must have the ability to

impersonate other authorized users for troubleshooting and tracking. In the event that data is changed by the super user impersonating another, the system must accurately record this activity in the audit log.

### 1.9.4  Data Management, Portability, and Interface Requirements

This section contains the requirements for the Relational Database Management System (RDBMS) used to control the primary data storage for all software components. Service Provider must recommend a RDBMS product or identify RDBMS products, which can be used in support of the Service Provider's software. Consideration of Database constraints:

1.9.4.1  Multi-Tasking - The RDBMS must permit simultaneous database access, permitting simultaneous access to files and queuing update requests at the record or field level when field contention prevents simultaneous updates. In addition, it must permit concurrent processing of batch and on-line jobs accessing the same data files and database.

1.9.4.2  Independence - The RDBMS must be independent of terminal type or transaction type and be able to be accessed from any terminal in the network.

1.9.4.3  Logging, Restart, and Recovery - The RDBMS must provide restart capabilities, as well as database access activity logging and blackout.

1.9.4.4  Performance and Activity Statistics - The RDBMS must support performance monitoring tools and activity statistics reporting features. Statistics should be available on database access rates (both update and query) by program, terminal, and ID, and by time of day.

1.9.4.5  Administrative Tools - The RDBMS should include a powerful set of administrative tools to monitor utilization, trace database access chains, optimize schema and sub-schema definitions, model, report areas/pages percent full, and to optimize file placement and layout.

1.9.4.6  Relational Database Characteristics - The RDBMS should utilize the concept of user views whereby pseudo-schema are defined and stored for utilization by users without the users becoming involved in the actual schema and sub-schema structures of the database. The system should provide a security system to control utilization of user views by user ID, account, and activity.

1.9.4.7  Data Dictionary Facility - The system should include an active integrated data dictionary. This dictionary should be an integral component of the data access capabilities, including the definition of both data attributes and values.

1.9.4.8  Data Import Facility - The system should include a data import facility which permits transferring data from other data files into the database.

### 1.9.5 Systems Interoperability Requirements

The system shall provide connectivity in real time or as nightly imports from other local law enforcement systems, many legacy platforms.

Preference shall be given to Vendors that can supply an API connector to all components of the provided system to allow for simple, secure access to these data in future. Vendor systems' must support outflow of data into other law enforcement systems.

1.9.6 TJJD seeks a Criminal Justice Information Service (CJIS) compliant environment. Service Provider must provide TJJD with a systems architecture design that demonstrates understanding of the sensitivity of the data and information maintained in the OMTS.

1.9.7 TJJD seeks a Health Insurance Portability and Accountability Act (HIPAA) compliant environment. Service Provider must provide TJJD with a systems architecture design that demonstrates understanding of the sensitivity of the data and information maintained in the OMTS.

1.9.8 Monitoring. Production environment and security infrastructure components that will be actively monitored 24x7x365 for performance, connectivity, and security. Alerts and alarms, as defined by TJJD, will be reported to TJJD, and Service Provider will participate in remediation efforts.

1.9.9 Evergreen Requirements. The versions of any software identified in this contract are to be considered the minimum versions. Service Provider shall provide a solution design that ensures that the OMTS is updated with current software releases.

1.9.10 API Integration that will allow authorized entities to obtain specific objects from a repository. The API service must provide the following:

- A standard method for interface to other Agency data services.
- A design that follows encryption standards as specified in the Federal Bureau of Investigation's Criminal Justice Information Services Security Policy (FB-CJIS).
- Designed and implemented based on JavaScript Object NationJSON and/or (REpresentational State Transfer (REST) standards.
- Includes a subscriber entity authorization and work flow.
- Data Integration points must include:
    - i. Activity Log

        1. Juvenile ID *(example: Booking Number, Jacket Number)*
        2. Juvenile First Name
        3. Juvenile Last Name
        4. DOB
        5. Race

6. Sex
7. Height
8. Weight
9. Hair Color
10. Eye Color
11. Housing Location

    ii.    Mugshot

1. Mugshot File *(formats: Binary, JPG, PNG)*
2. Mugshot Date Created
3. Juvenile ID

    iii.    Restrictions

1. Restriction ID
2. Restriction Code *(example: Suicide, Medical, Vegan)*
3. Restriction Start Date Time
4. Restriction End Date Time
5. Restriction Created By

    iv.    Keep Separates

1. Keep Separate ID
2. Keep Separate Juvenile ID
3. Keep Separate From Juvenile ID
4. Keep Separate Start Date/Time
5. Keep Separate End Date/Time
6. Keep Separate Created By

1.9.11 Security Requirements. Service Provider will work with TJJD technical staff to define and configure the technical environment in alignment with the requirements as stated in Title 1, Part 10, Chapter 202 of the Texas Administrative Code.

1.9.12 The application must be hosted in a Criminal Justice Information System (CJIS)-compliant physical environment and is requiring all technical documentation and/or data to be maintained in accordance with "CJIS Security Standards," this includes, but is not limited to, the hardware to be situated in a climate controlled, fault-tolerant environment complete with fire suppression, redundant power, cooling cabinets, and restricted personnel access.

1.9.13 Employees of solution provider may be required to complete TJJD approved background check process and any who will have specific access to the data in this system may be

required to undergo agency background checks. Sensitive data must be encrypted at rest and in transit.

## 2    DELIVERABLES

1.  **Service Provider shall develop or configure, test, stage, and release business applications by applying iterative processes utilizing the proposed Agile methodology and a frequent release cycle.**

2.  Deliverables must be provided on the dates specified. Any changes to the delivery date must have prior approval (in writing) by TJJD project manager or designate.

3.  All deliverables must be submitted in a format approved by TJJD project manager.

4.  If the deliverable cannot be provided within the scheduled timeframe, Service Provider is required to contact TJJD project manager in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

5.  A request for a revised schedule must be reviewed and approved by TJJD project manager before placed in effect. Contract Terms and Conditions may dictate remedies, costs, and other actions based on the facts related to the request for a revised schedule.

6.  TJJD will complete a review of each submitted deliverable within 5 working days from the date of receipt unless otherwise stated by TJJD.

7.  Relevant quality assurance processes that will apply, such as change management, acceptance, and risk and issue management. Service Provider will utilize an agreed upon Project Management methodology.

8.  Provide the necessary access to TJJD staff to all development environments, including sandbox, testing, and productions environments.

### 2.1    Project Milestones

#### 2.1.1    Kickoff Meeting

A kickoff meeting will be held at a location and time selected by TJJD where the Service Provider and its staff will be introduced to TJJD. Service Provider shall submit kickoff meeting notes within five business days after the kickoff meeting that documents all topics discussed during the meeting.

#### 2.1.2    Project Management Plan

Service Provider shall submit an initial project management plan to TJJD. Additionally, within 10 business days after the kickoff meeting, the plan should be updated to document how the Service Provider plans to facilitate project management activities going forward. Both the draft and updated project plan associated with this effort shall include adequate

information to establish team members, meetings/workshops schedule and resource management. At minimum, the plan must include:

2.1.2.1  Provide the project management approach for this effort.

2.1.2.2  Provide an overall project schedule that includes anticipated duration dates, resources, dependencies, and milestones for each project phase and task.

2.1.2.3  Service Provider's summary of deliverables required  and any additional deliverable the Service Provider plans to execute this effort is included in Exhibit A, Project Plan.

2.1.2.4  Identify specific skills to be provided by the Service Provider, skills/resources TJJD is required to provide, and expectations of TJJD staff time commitment.

2.1.2.5  Provide a staffing management plan including how the project will be staffed with all Key Personnel, a summary of strategic partnerships (subcontractors), and the approach for managing subcontractors..

2.1.2.6  Identify any assumptions and risks for executing this project.

2.1.2.7  Provide proposed work location where data collection would occur.

**2.1.2.8  Project Work Plan**

Service Provider's drafted high-level project work plan addressing the tasks specified in the contract and is representative of the analysis of the source code provided, including:
- A description of key activities and milestones.
- A description of the Service Provider's working documents, deliverable, or component technologies completed for each sprint/iteration.
- A description of the resources necessary from TJJD to support the sprint.
- List any assumptions and dependencies of the project.


**2.1.3  Reports and Meetings**

1. The Service Provider is required to provide the TJJD project manager with weekly written progress reports of this project. These are due to TJJD project manager by the close of business on Friday each week throughout the life of the project.

2. The progress reports shall cover all work performed and completed during the week for which the progress report is provided and shall present the work to be performed during the subsequent week.

3. The progress report shall identify any problems encountered or still outstanding with an explanation of the cause and resolution of the problem or how the problem will be resolved.

4. The Service Provider will be responsible for conducting weekly status meetings with TJJD project manager. The meetings will be held at a time and place so designated by TJJD project

manager. The meetings can be in person or over the phone at the discretion of TJJD project manager.

### 2.1.4 Testing and User Acceptance Plan

Agile projects require that the Product Owner (the Agency for this project), identify specific and unique criteria for determining whether a User Story performs as expected. For each Sprint, the Service Provider shall develop user stories specifications that include use cases, narrative text, story test, acceptance criteria and any business rules and assumptions that apply to aid the proper configuration of the software to deliver the expected functional outcome. At the end of each Sprint, the Product Owner will review planned deliverables as either Done or Not Done.

### 2.1.5 Administration Documentation

1. System Manual - System shall have the availability of a detailed, on-line system manual with guides for various user roles (e.g., system technical personnel, system administrators, end users, etc.).

2. Changes - Service Provider shall have and implement methods for streamlined changes to the system and corresponding documentation.

3. System and Business Requirements - Service Provider shall provide staffing to work in collaboration with TJJD employees to document both system and business requirements, as well as test plans, scenarios, and scripts.

4. Reported Problems - Service Provider shall document, track and report problems, change requests and bugs and the resolution of such. Service Provider shall follow a standard set of steps until problems and bugs are corrected and change requests are completed. The Service Provider shall provide escalation procedures. Service Provider shall assign incident numbers to all such reports and queries and shall maintain these incidents in a tracking database.

### 2.1.6 Implementation Plan

1. Planning and Discovery Phase - Service Provider must provide a realistic but aggressive discovery and planning timeline. The steps necessary for this phase must be laid out by the Service Provider. A full implementation plan shall be required to be developed by the Service Provider in collaboration with TJJD.

2. Implementation Phase - Service Provider must provide a realistic but aggressive implementation timeline. Implementation plans shall be provided in draft form based upon the Service Provider's past experience and recommendations. A phased implementation plan shall be considered suitable with sufficient reasoning provided by the Service Provider.

   A detailed project implementation plan in MS Project or State/Agency approved equivalent is to be provided as follows:

   a.   Configuration: Preliminary system modification/development plan
   b.   Customization Plan
   c.   Data Configuration and Implementation Plan

d. An Interface Control Document (ICD) for each interface listed in the contract. This document will describe the functional requirements and data elements for each interface to such level that ambiguity is reduced to a minimum.
e. Preliminary functional acceptance test plan for the applications and interfaces
f. Preliminary system performance test plan
g. Training Plan: Preliminary training, training documentation, data conversion
h. Cutover plan: high-level plan

### 2.1.7 Training Program and Plan

The Service Provider provided a training program and plan document as part of their proposal response. The training plan shall include the following items and any additional components as offered by the Service Provider. Training programs shall consist of in-person group trainings and may also entail web based trainings to supplement in-person training sessions.

1. <u>End-User Training</u> - Customized training for the TJJD staff who shall be using the system for internal support, customization, and optimization.

2. <u>Administrator Training</u> - Customized training for TJJD staff who shall be administering the system for internal support, customization, and optimization.

3. <u>Supervisor Staff Training</u> - For mid-level supervisors to manage their staff and juvenile loads optimally, the supervisors shall have oversight of the system for specific Units only.

4. <u>Data/Research/Analyst Staff Training</u> - For internal staff who are responsible for analysis and data management, research, and quality assurance.

5. <u>Senior Executive Staff Training</u> - Trainings for senior staff who shall require system overview abilities.

6. <u>Online Training</u> - Trainings using text, graphics, and video must be provided for real time guidance and training on new topics.

7. <u>Training Plan</u> – The training plan shall include:

    a. A synopsis of the overall training (e.g., objectives, content overview, recommended class size, estimated length of classes, etc.).
    b. A syllabus of all proposed training including class descriptions and durations.

c. Description of training environment and method of instruction (e.g., learning environment setting(s) and methods to engage learners, etc.).

d. The intended audience (e.g., role-based, function based, external users, internal users, etc.).

e. The source of the training (e.g., Vendor supplied or 3rd party supplied).

f. Student prerequisites for each course, if required.

g. Training schedule.

h. Training time availability: Institutional staff require trainings during evenings and weekends. The Service Provider shall state if evening and weekend trainings shall be made available and if there are any limitations.

i. Training Documentation: Service Provider have training documentation provided and state if there shall be an On-Line User Guide by function/module.

j. On-going Training and Documentation: Service Provider shall state how all users, from system technical personnel to user personnel, shall be trained and kept current with system updates, version changes, and new applications. Service Provider shall state how training materials shall be updated to reflect changes.

## 2.2 Support

Service Provider shall offer a comprehensive support package to TJJD for the duration of the contract. This support shall include the following:

1. Live Web Based Support - Service Provider shall provide a web based chat style support feature to allow users to connect with available support personnel simply and quickly. The Service Provider should outline and specify the support options.

2. Phone and Email Based Support - Service Provider shall provide phone based support for users at the supervisor level and below with a ticket based system guaranteeing four (4) hour response times and shall be available daily from 7:00 am through 6:00 pm CDT. For infrastructure support staff this response time must be guaranteed at two (2) hours and shall be available 24 hours per day 7 days a week.

3. Web Based Support - Service Provider shall provide a web based support portal allowing users to submit requests and track them live.

4. System Updates - Any system updates and changes to the system shall be pushed out to the users in coordination with TJJD's change advisory board procedures. Service Provider staff must be available for the initial integration of new functionality and updated training tools and support shall be provided during these times.

## 2.3 Maintenance

1. System Guarantee - Service Provider shall provide an overview of their plan to provide a maintenance and upgrade plan to support the functions outlined in this contract for the entirety of the contract. Any defects and malfunctions identified shall be fixed and patched by Service Provider at no additional cost to TJJD and in an expedited timeframe unless determined to be a minor flaw with minimal operational impact.

2. System Updates - Service Provider shall provide a system that is configurable to allow for the addition of new functionality or related fields as outlined by code or by legislative act at least annually, at the beginning of the calendar/fiscal year, and upon request by TJJD, as laws, penal codes and other reporting codes or business processes or changed.

3. Evergreen Requirements. The versions of any software identified in the contract are to be considered the minimum desirable version. Service Provider will provide for TJJD to receive updates to current software releases and maintain a hardware refresh cycle of at least 3 years per device for component devices required to implement the OMTS.

## 2.4 Service Level Agreement

Service Provider will establish and maintain Help Desk Support for all provided components related to the application and environment, which includes:

(i)  Diagnosis of problems or performance deficiencies of the system;

(ii)  A recommended resolution to the reported problem or performance deficiency; and

(iii)  Close coordination between development resources and TJJD technical staff regarding any testing and/or implementation of corrective actions. Service Provider will provide primary telephone software support on a daily basis during standard business hours (8:00 am - 5:00 pm) and will provide after-hours support via e-mail. After hours support is defined as response by e-mail within 4 hours on weekdays between the hours of 5:00 pm and 8:00 am and within 6 hours on weekends and official state holidays. Service Provider will ensure any reported/identified defects within the system are documented, assessed, and a recommended solution is defined. All issues must be tracked as part of a comprehensive ticket management system. Escalation procedures and timelines will be determined collaboratively between Service Provider and TJJD.

a. Service Provider shall establish and participate in regularly scheduled problem management meetings with TJJD technical staff to review new and existing issues and to develop a remediation plan commensurate with the severity of the identified issue(s).

b. Incident Management. In conjunction with TJJD's existing Help Desk Services, Service Provider must be able to diagnose and correct defects in the production environment, both technical and application related, in accordance with the following service levels:

   i. **Severity Level 1 – Critical**, defined as a problem or outage that directly impedes a user's ability to carry out essential business functions.
      A. Response will be provided within two (2) hours for all Severity Level 1 issues.
      B. Resolution by continuous work until resolved by either permanent fix or temporary fix that allows the user to resume essential business functions.
   ii. **Severity Level 2 – Urgent**, defined as an issue or problem that hampers a user's ability to utilize a specific function within the system but does not prevent TJJD from carrying out essential business functions; deemed a high-priority item for attention.
      A. Response will be provided within two (2) calendar days for all Severity Level 2 issues.
      B. Resolution by continuous work until resolved with either a temporary fix or patch or permanent resolution that allows the user to resume normal operation of essential business functions.
   iii. **Severity Level 3 – Normal**, defined as a defect or issue that, if corrected, would improve the use or functionality of the system. Deemed as a low priority.
      A. Response provided within five (5) business days for all Severity Level 3 issues.
      B. Resolution based on joint planning to determine when to apply temporary fix or patch or to implement a permanent solution to address issue.

c. TJJD will make necessary initial decisions to interpret severity levels and service levels. The Service Provider will have the authority to request a conference, to occur as expeditiously as reasonably possible. The conference will be between representatives of the Service Provider and TJJD, and will be for the purpose of

discussing the severity level or service determination and attempting to resolve the disagreement.

## 2.5 Issue Tracking & Support.

a.  Service Provider will ensure that a defect and issue tracking system is utilized to capture and track actions taken for reported issues and defects.

b.  Service Provider shall track and analyze reported functional and technical defects or issues, work to identify the root cause, **and** develop/implement needed modifications to mitigate the reported issue.

c.  TJJD staff will be provided access to record information about identified defects and issues and to review progress regarding such reported issues.

d.  Service Provider will undertake all reasonable efforts to provide technical assistance under the agreement and to rectify or provide solutions to problems where the system does not function as described in the system documentation.

e.  Service Provider will provide skilled technicians to support both server and networking components.

## 3  INVOICES

Service Provider will submit invoices to TJJD Claims Department via email at tjjdinvoice@tjjd.texas.gov and/or via regular mail at, 11209 Metric Boulevard, Building H, Suite A, Austin, Texas 78758, on invoices bearing Service Provider 's name, address, and TJJD contract number. Invoices will be submitted not less than thirty (30) days prior to the payment due date. Yearly payment will be due on the anniversary of the first facility's go-live date. Payments will be made in accordance with Chapter 2251 of the Texas Government Code.

## SECTION III: TJJD

TJJD will pay Service Provider a fee for the develop/configure, test, stage, and release a OMTS solution for all of the site locations. The not-to-exceed amount for this contact for the two-year term is **five hundred eight thousand, four hundred ten dollars and thirty-nine cents ($508,410.39): four hundred forty-four thousand, four hundred ($444,445.39) in year one; and sixty-three thousand, nine hundred sixty-five ($63,965.00) in year two.** Payments will be made in accordance with Chapter 2251 of the Texas Government Code.

## SECTION IV: NOTICES AND CONTACTS

Notices shall be addressed to the Office of General Counsel, Texas Juvenile Justice Department, mailing address: P.O. Box 12757, Austin, Texas 78711; or physical address: 11209 Metric Blvd., Bldg. H, Ste. A, Austin, Texas 78758, and to Service Provider at 1705 Crossing Place, 101A, Austin, Texas 78741. The following is additional contact information for purposes of this contract:

| Service Provider Contact Information: | TJJD Contact for Technical: |
|---|---|
| Melynda Caudle | Virginia Miller, Chief Information Officer |
| President | 11209 Metric Blvd, Bldg. H, Suite A |
| 1705 Crossing Place, 101A | Austin, Texas 78758 |
| Austin, Texas 78741 | Phone: 512-490-7287 |
| Phone: 512-527-1000 | Fax: 512-490-7252 |
| Fax: 512-527-1001 | Email: Virginia.Miller@tjjd.texas.gov |
| Email: caudle@cooperconsulting.com | |
| **Service Provider Subcontractor Contact:** | |
| Name: Ken Dalley, Jr. | |
| Phone: 855-777-7343 | |
| Fax: 877-842-6339 | |
| Email: ken.dalley.jr@guardianrfid.com | |

## SECTION V: CERTIFICATIONS AND GENERAL PROVISIONS

**TJJD's Certifications and General Provisions are attached hereto as Exhibit C and hereby incorporated by reference. If any of the terms and conditions in the Certifications and General Provisions sections conflict with any of the terms and conditions of Service Provider's contract with the Texas Department of Information Resources (DIR), the terms and conditions of Service Provider's DIR contract take precedence.**

**COUNTERPARTS.** This contract may be executed in counterparts, each of which shall be deemed to be an original, and all of which taken together shall constitute one and the same instrument.

**IN WITNESS WHEREOF**, the parties hereto have made and executed this contract as of the day and year first written above.

**For the Texas Juvenile Justice Department:**

_Mannys for Camille Cain_      3/29/2019

Camille Cain, Executive Director           Date

**For Cooper Consulting, Company (Service Provider):**

_Melynda B. Caudle_   MELYNDA B. Caudle   8/29/19

Signature           Printed Name          Date

**Approved as to form:**

                                                 8/29/19

TJJD Attorney           Date

# EXHIBIT A

# TAB 2 – Project Plan

*In this Tab the Vendor shall provide a description of the proposed services in detail. Vendor shall provide a detailed description or summary of its service performance on the specification in this solicitation in the following sections:*

# Section 1 – Understanding of the Project

*The Vendor shall provide a narrative on their entire understanding of project as described in this RFO. The narrative should include how the Vendor is the best positioned to perform the tasks of this project based their corporate organizational structure, overall experience and past performance developing and deploying similar solutions to what the Agency is requiring.*

Corrections professionals have always been - and will always be - the most underserved segment of law enforcement. They are often an afterthought when it comes to technology and budget, and yet they are one of the most critical and responsive forces behind the law. Experts in emotional intelligence, they know how to be firm, fair, and consistent with the country's toughest individuals. They strive tirelessly to protect the well-being of those who wish harm upon themselves and others. Corrections professionals are met with ingratitude both inside and outside the walls of their facility.

The Cooper team with GUARDIAN RFID proudly stands for corrections professionals.

TJJD wants a solution that will help their officers log more in less time so as to achieve legal defensibility and prove no deliberate indifference toward its youth offenders. The TJJD has increased its operational efficiency over the years when it comes to processing and closing complaints and incidents. However, the influx of complaints is also increasing. During last quarter alone the OIO received 19 complaints, which represents a 58.3% increase when compared to the second quarter of FY 18. Complaints received during youth interviews increased by 100% when compared to the second quarter of FY 18. (Office of Independent Ombudsman, Q2 2019 Report). The TJJD team is also seeking new ways to routinely battle drug trafficking (McLennan) as well as infrastructure deficiencies (Gainesville).

The scope of this project is to improve event logging, not to simply make the officer's life easier but to make officers more effective. The more officers document, the more legally defensible the team will be. TJJD is seeking a logging solution that is mobile and reportable.

**Mobility**
Officers assigned the daily tasks of a direct supervision pod are walking by cells, looking in windows, and then going back to their workstation to document what they saw based on their memory. Officers can't accurately remember and document everything they saw by memory, especially when bombarded with questions and requests by offenders.

Mobile solutions solve all that by putting the computer in the officers' hands while room checks are being completed. They can document at the point of responsibility, making sure that logged information is accurate and not sparing any detail. The chances of forgetting a detail if you're documenting while you're standing in front of the cell is significantly smaller than when you're back at your computer workstation 20 individual cell checks later.

Not only does manual computer entry require staff to document based on memory, but it also forces officers to focus their attention on a screen rather than the offenders. Administration wants computer generated logs, but they also want their officers to be engaged and having face-to-face contact with offenders. Less officer/offender interaction means less observations, ultimately decreasing the number of detailed notes within the logs.

Mobile inmate tracking is just that: mobile. Staff can track and log offender well-being while looking at youth offenders during the cell checks, not afterwards when they're in front of a computer.

For facilities using only hand-written logs, spelling errors, incorrect grammar, and chicken scratch are all common issues. If the notes are illegible or incorrect, it's difficult to be legally defensible in court or dispute youth complaints. Some agencies attempt to solve these problems by having line staff type notes into their offender management system (OMS). Those are only going to be accurate if every officer gets enough face-to-face interaction with youth offenders, remembers absolutely everything they observed, and want to take the time to manually type every notation into the OMS.

Administrators who use paper logs are painfully familiar with pencil whipping. Security check logs that are perfectly 30 minutes apart on the minute, the word "same" row after row. Pencil whipping becomes impossible with a mobile solution because you can't backdate an RFID chip that is drilled into cinder block. It's much easier and more accurate to simply talk into your mobile device or tap pre-defined behavioral descriptions to take notes while looking at the youth while compete the cell checks.

**Reportable**
Event logs, whether electronic or otherwise, exist to be viewed and consumed by the administration, agencies, and the court. The information collected should be accessible to administration immediately, being able to draw insights about the past at any time and from any device.

With paper logs, agencies have to rely on a recordkeeper to pull all necessary documentation. Administration then has to sift through the big stack of paperwork for what they truly need and then turn all that paper into a tidy summary for the agency or judge. The process is time consuming, inefficient, and doesn't easily provide insights.

If using a cloud or web-based local host, all administration has to do is go to the computer and generate a report. Some cloud and web-based platforms produce reports better and faster than others, but they're all significantly better than searching through boxes of paper. Pulling insights is much easier to do on a computer. It can compile all collected data and display insights such as the facility's compliance percentage. The levels of insights will differ depending on the specific platform being used.

TJJD is seeking an event logging solution for all of its offender-specific logs. If staff start capturing all logs on mobile, and if administration are given real-time access to these logs, then the TJJD will start to see a decrease in complaints. The Cooper Team with GUARDIAN RFID have seen this phenomenon in pre-trial facilities across the country; when inmates see that every aspect of their day is meticulously tracked then they think twice before filing a complaint - if nothing else to simply save face.

Offender-specific logs include, but are not limited to:
- Proof of presence checks

- Special watch / well-being observations

- Out-of-room movements

- Shakedowns / room search

- Headcount

- Supply passes

- Med passes

- Keep separate flagging

- Religious restriction flagging

- Allergy restriction flagging

- Special watch flagging

- Use of confinement logs

- Meal passes / refusals

- Recreation access / refusals

The Cooper team with GUARDIAN RFID counts on first-hand corrections experience to design, deploy, and scale Cloud-based offender tracking systems. The company's solutions have been adopted by over 32 states, currently supports 15,000 end users,

and captures 1 billion activity logs per year. TJJD can count on Cooper and GUARDIAN RFID to deliver a proven solution for the scope of this project.

# Section 2 – Proposed Solution

*The Vendor shall provide a narrative on their proposed solution that demonstrates how their solution meets all of the technical and functional requirements as specified in this RFO. The Vendor must indicate which technical or functional requirements their proposed solution does not meet. The Vendor shall not submit marketing materials as the narrative for this section; however, the Vendor may include marketing materials as appendices to their proposal.*

## Technical Requirements

## General System Capabilities

### Log Movements

The Cooper Team with GUARDIAN RFID proposes a youth tracking solution that will be entirely mobile; a solution that does not require staff to return to a computer workstation in order to log an offender's movement. When a youth is scheduled to move to a specific destination, staff will simply pull a mobile device from their utility belt, scan an RFID chip (wall-mounted at the housing unit) and tap a predefined destination on their screen. This will log the timestamp, staff, youth, place of origin, and expected destination.

### Pull Movement Reports

The Cooper Team with GUARDIAN RFID proposes a simple, robust data repository to contain the movement history of each and every youth. While staff use their mobile device to track youth movements throughout the day, all their logs will be instantly synced to a centralized data repository (cloud hosted). Supervisors and command staff will have access to this data repository through a simple user interface, with the ability to filter by date, time, staff member, youth name, youth ID, destination, and place of origin. Each youth record will form a chronological string of events from booking to release. Youth movement history will be stored in perpetuity on the data repository for future reporting.

### Notify Staff About Movements

We propose a dynamic list that allows staff to see movement queues directly on their mobile device. The mobile device will display a subtle notification icon on the main screen informing the user that specific youth are destined for a location such as programs, recreation or court. This notification will be targeted to ensure that only relevant lists are shared; staff will only see youth for whom they are directly responsible.

### Log Observations

We propose a solution that captures extensive observations during well-being checks. This solution will be purely mobile so as to ensure that staff are face-to-face with youth when logging

observations. When officers are conducting their well-being checks they will use their mobile device to:

1. Scan wall-mounted RFID chips (this will display a list of offenders in that area)

2. Select one or many offenders on their screen

3. Tap on predefined observations (example: chest rising and falling, appears asleep, etc.)

## Receive Alerts (Real-Time)

GUARDIAN RFID proposes a mobile solution that will be entirely real-time. All logs captured by this mobile application will be instantly synced to a centralized database (cloud hosted) where they will be available to supervisors in real-time - within two seconds of capture. As it relates to officer rounds, all proof-of-presence rounds will be instantly uploaded to the cloud, allowing a separate web application to display real-time dashboards with audible and visual "late check" alerts.

## Integrate Into Existing Enterprise Ecosystem

The Cooper Team will allocate an in-house developer to TJJD for the creation and sustenance of a RestAPI. This API will be available to TJJD to call at any desired interval. Payload sizes will be throttled to ensure that any given request does not crash the cloud server. We suggest that TJJD implement a methodical (2-5 minute) pull request as opposed to large one-time requests.

## Customize Workflows

We propose a solution that can be customized and tailored without the involvement of vendor support. All software created by the Cooper Team (whether mobile or web) will take a modular approach, meaning that command staff will have the ability to easily create mobile screens for officers, so as to help validate data entry. Each new mobile module will instantly generate a canned report on a separate web application.

## Monitor Compliance (Real-Time)

We propose a monitoring system that maps to each location in TJJD's offender management system. TJJD will send the system an updated offender roster every 3-5 minutes. This roster will be a .csv file containing the following fields: [Youth ID], [Youth Name], [Housing Assignment], and [Special Statuses]. The system will ensure that each youth is represented in the mobile and web application, and the system will ensure that each location has a "max check time", thus ensuring that officers receive alerts to check on each offender every [max check time] minutes. Offenders will be grouped together by common housing units so that officers may receive alerts on their mobile app and web dashboards. Command staff will have the ability to update the max check times on a location at any time through the web app.

## Pull Observation Reports

We propose a web reporting system that allows supervisors to access any log on the central data repository (cloud hosted). Supervisors will be able to access these reports from any device with internet connectivity, using their unique login credentials. The reporting system will allow for instant querying of logs by: date, time, staff, youth, keyword, workflow module, etc. In addition to these filters, the supervisor will be able to display photos that may have been captured during the mobile logging process.

## Distinguish Between Active/Inactive Youth                          3.1.11

The system will ensure that its interface with the TJJD offender management system has the necessary triggers to delay the release of youth based on specific time/classification criteria. The solution proposes retaining all logs and youth profiles in perpetuity and plans on offering TJJD unlimited storage within the data repository (cloud hosted).

## Integrate Special Watch Into Compliance Monitor                    3.1.12

The system will ensure that its interface with the TJJD offender management system includes all special statuses relevant for legal defensibility. Suicide watches will follow youth wherever they are housed or moved, which means that staff can be alerted to scan their wall mounted RFID chip at least every 15 minutes as long as the suicide watch status is active. This status will be communicated to the officer in a discreet manner to ensure that offenders do not inadvertently discover the status. Other special statuses such as religious restrictions, keep separates, and allergy restrictions will also be integrated into the system.

# Component Devices Requirements

## Tag Locations With RFID

The Cooper Team proposes a low maintenance RFID chip with a durable enclosure. This RFID chip will be compatible with standard NFC hardware present in today's consumer grade mobile devices (13.56Ghz). The Cooper Team will provide a custom molded enclosure that is waterproof and can withstand blunt force strikes. This solution will leverage passive RFID technology, so as not to require batteries or wiring of any kind. This RFID tag will drill directly into the cinder block near housing units, allowing staff to scan the tags with their mobile devices. Each RFID tag will represent a unique ID on the mobile devices database, allowing the mobile device to display lists of youth for various workflows, including well-being checks, supply passes, headcount, etc.

## Track Staff Accountability

3.3.2

The Cooper Team will create a user access management portal on a web application that will allow command staff to create, modify, and delete users. This portal will offer command staff the ability to grant and revoke specific permissions to officers. This portal will allow command staff to update usernames and passwords. All credentials will apply to both mobile and web.

## Agile & Scalable Deployment

3.3.3

We propose a solution that maps to the housing structure already present in TJJD's enterprise systems. When new locations are created within other TJJD systems, command staff will be able to log into the system web portal and map new locations without the involvement of vendor support.

## Durable Mobile Device

3.3.4

We propose a logging solution that will be entirely mobile and cloud focused. Staff will have the ability to use a mobile device to log any youth activity throughout the day. This mobile focus will ensure that officers keep their eyes on the offenders during the logging process, instead of glued to computer screens. The Cooper Team will coordinate the provisioning and programming of a mobile device that meets the following minimum requirements:

- Operating Temp up to 133°F

- Storage Temp up to 150°F

- Drop Spec up to 8 feet on concrete (MIL-STD 810G)

- Battery life up to 18 hours (battery no larger than 6400mah)

- Hot swappable battery

# Electronic Log Requirements

## Log Officer Rounds

We propose a mobile app that proves the physical presence of officers at each significant step of their security round. Preferred workflow:

1. Officer logs into mobile device with badge number,

2. Walks past locations of interest and scans the wall-mounted RFID tags,

3. Saves check once the round is complete.

All logs will instantly sync to a central data repository (cloud hosted) so that officers will have real-time alerts about upcoming rounds. Each RFID tag will have a specific "max check time" defined by command staff and youth special status.

## Log Room Checks

We propose a mobile app that allows staff to quickly log meaningful observations about youth well-being, without taking their eyes off the youth. Preferred workflow:

1. Officer walks past locations of interest and scans a wall-mounted RFID tag,

2. Taps on one or many inmates in the location,

3. Taps on one or many predefined observations.

In addition to these predefined observations, the system will provide consumer-grade voice transcription technology so that officers will be able to speak observations out loud without taking eyes off the youth.

## Record Movements

We propose a mobile app that allows staff to capture movements on mobile so as to create an unbreakable chain of movement history on the web for each youth.

Preferred workflow:

1. Officer scans a wall-mounted RFID tag,

2. Taps on one or many inmates in the location,

3. Taps on one or many predefined destinations.

All movement logs will be logged on the web for historic reporting but also be available at the point of responsibility through mobile so that staff have an ongoing list of offenders (both where they are housed as well as their out-of-cell location).

*NOTE: The Cooper Team would also entertain RFID Wristbands as an alternative workflow.*

## Log Meal Service

We propose a mobile app that allows staff to capture meal refusals.

1. Officer scans a wall-mounted RFID tag,

2. Taps "accept" or "decline" on the screen next to each offender's name,

3. Hits a Save button once all offenders have been offered a meal.

Whenever a youth declines a meal, the mobile app should allow the officer to leave annotations regarding the youth's well-being, for example: stomach ache, hunger strike, religious abstainment, etc.

*NOTE: This same workflow may be followed for recreation instead of meals.*

## Log Med Passes

We propose a mobile app that logs medication administration to each youth, generating eMAR reports on the web app. Preferred workflow:

1. Officer scans a wall-mounted RFID tag,

2. Taps the name of a youth with a due medication

3. Logs "accept" or "decline" and then captures a signature.

Nurses will have the ability to create these medications, complete with dosage, route, schedule and special notes.

## Clear Count

We propose a mobile app that allows staff to account for each youth offender in the entire facility - or part of the facility. Preferred workflow:

1. Officer scans a wall-mounted RFID tag,

2. Taps "present" or "not present" on the screen next to each offender's name,

3. Hits a Save button once all offenders have been offered a meal.

The system will ensure that all offenders are assigned to the correct housing units based on its interface with TJJD's offender management system. We will build in an out-of-cell feature into this headcount workflow to ensure that out-of-cell offenders are mapped to the correct RFID tags.

# Business Rules Validation Requirements

## Dictate Workflow Steps

We propose a set of data validations that are can be easily curated by command staff without the involvement of vendor support. Examples of mobile data validation might include:

- Require staff to use [#] predefined observations at [location] in order to satisfy compliance monitor

- Remove [location] from compliance monitor when no youth is assigned to the room

- Prevent mobile user from offering any offender more than [#] recreation sessions per day

- Prevent mobile user from logging movement if keep separate rule exists

- Remind mobile user of [special status] when [RFID tag] is scanned

## Validate Data Entry

We follow today's UX best practices to ensure that the web application (.net preferred) validates user input and safeguards database integrity. To ensure user-friendliness, all column headers will have a hover-over tooltip explaining the valid input.

## Lock Past Logs

Our team has been creating offender tracking platforms for over 14 years, for this reason we are well aware of the type of lawsuits and grievances that correctional agencies face. We will ensure that no staff (not even command staff) ever have the ability to modify or delete any log. If a log is ever erroneously captured, then staff will have the ability to append a note to that log, but never purge it. This will ensure the integrity of each facility's event logs - establishing a legally defensible body of evidence that each TJJD facility can confidently defend in court.

## Manage User Access

We will implement best-in-class user access management principles to ensure that command staff have the ability to curate platform access (both mobile and web). User roles will be distinguished based on workflow, user group, user role, and temporary permission set.

# Logs Requirements

## Pull Offender-Specific History

We propose a data repository with unlimited concurrent users, unlimited storage, and perpetual retaining of data. Every event log captured with the mobile app will be stored on the cloud and accessible through a user interface. This user interface will allow staff to pull exhaustive reports on named youth (including previous bookings), named mobile users, or specific housing units. All logs are captured with the goal of legal defensibility.

## Classify Housing Units

3.6.2

We will ensure that command staff have the ability to tailor each housing location to the classification of the offenders therein contained. Command staff will have the ability to set a location to high, medium or low risk for the purposes of well-being checks. Schedules and workflow restrictions will be available parameters while managing housing areas on the web portal.

## Audit Users

3.6.3

We will retain a historical usage report on all end users, including login history, record creation history, permission modifications, admin parameter changes, etc. These audit reports will be available to select Super Users on the web portal.

## Restrict Records By Youth

3.6.4, 3.6.5

We will provide advanced data analytics capabilities that will allow command staff to manipulate data visualizations and create restricted views for external users. These dashboards will feature calculated fields that prevent certain fields and data points from appearing on data visualizations.

## Document Refusals

3.6.6

We propose a mobile app that facilitates the logging of accepts and refusals. These attributes will apply to workflows such as: recreation, meals, medications, etc. In addition to tracking each offender's acceptance or refusal, the system will leverage mobile hardware to capture signature and photo.

## Manage Person/Resource Profiles

3.6.7

We propose a web application that allows command staff to define profiles for both individuals and resources. Offender Profiles will support validated demographic fields (e.g.: Race, Religion, Control Agency) and special status flags (e.g.: Kosher, 2-Man Escort, Vegan). Officer Profiles will support permission sets as well as credential definition. Resource Profiles will support the creation of asset attributes so as to track the condition or depletion of assets over time - resources might include: fire extinguishers, SERT closet, and breathing equipment.

## Institute Inspection Rules

3.6.8

We will ensure that command staff have the ability to define the round compliance of each housing location. Command staff will have the ability to require observations on certain areas to ensure legal defensibility. Certain posts and locations will also be designated as Supervisor Rounds to ensure that supervisors visit each housing unit during their shifts.

## Send Targeted Notifications

3.6.9, 3.6.10

We propose push notifications and popup messages that appear on the mobile app. Examples of mobile notifications include:

- Violation of youth-on-youth keep separate rule

- Notice that youth cannot be moved while in the possession of nail clippers or razor

- Notice that medications are due within [#] minutes

- Notice that youth may only receive [#] of a particular item

- Notice that youth is on [special status] prior to interaction

We will discover the business requirements of each TJJD facility and tailor its alerts to the policies and procedures of each team. We will support mobile and web alerts as well as email notifications (cannot guarantee SMTP integration).

## Empower End Users

3.6.11

We propose a mobile solution that empowers frontline officers to create special statuses at the point of responsibility so as to streamline communication. Officers will have the ability to scan an RFID tag, select a youth and apply a predefined special status. These special statuses will trigger relevant warnings to other end users. Notifications may be applied to named youth and/or specific locations.

## Expand Navigation & Parameters

3.6.12

We will ensure that all log reports be easily navigable with a user-friendly dropdown menu and tree diagram. Whether staff are accessing a compliance monitor dashboard or pulling a historical report, they will have the ability to easily expand and collapse locations in a logical fashion. While creating notification parameters, the user will have the ability to expand a specific notification parameter (example: alert staff every 15 minutes to check [location] if occupied) to several locations.

# Health Services Monitoring Requirements

## Update Medication Attributes

We will allow any given medication to bare attributes controlled by special status. Based on certain offender classifications, a medication will be flagged differently to end users to indicate attributes including: carry/non-carry, formulary/non-formulary, narcotic, restricted, etc.

## Expand Offender Profile

3.7.2

We propose a modern mobile UI that will feature the offender's profile thumbnail whenever their name is displayed on the screen. During med passes, this thumbnail will appear next to the due medication, and the thumbnail will allow a tap-to-drill down feature that will open up the youth's full profile if the user so desires.

## Prioritize Offender Lists

3.7.3,
3.7.4

We propose a set of manual, as well as automatic, sorting abilities. When a list of medications/offenders appears on any mobile screen, the end user will have the option of manually sorting by name or housing location. However, by default the application should sort by medication due time so that the nurse or officer proceed according to urgency. These lists may represent either due medications or due services depending on nurse-defined schedules.

## Create Special Medical Workflows

3.7.5

We propose separate mobile workflows for approved devices and special appointments. Each workflow will have variable lists that nurses can define through the website. All lists created on the website will flow into mobile so that mobile users can track the issuance and retrieval of devices as well as the start and finish of special appointments.

## Distinguish Infirmary Locations

3.7.6

We propose that nurses leverage the same location schema that will be used by command staff to designate special watches and round compliance. All locations within the facility - including the infirmary - will appear on the GUARDIAN RFID schema and will receive updated rosters through its interface with the offender management system.

## List Youth Medications

3.7.7

We propose a repository that can store descriptions of each offender's medication. Lists will include both active and inactive medications and will allow staff to run pill audits over time.

### Create Medication Orders

We propose a web application exclusively used by nursing staff. This platform will allow nurses to create medication orders for specific offenders, complete with date ranges route, dosage, unit measures, special instructions, frequency, etc. Tapers can be created by configuring date ranges and frequency parameters.

### Medication Adjustments

We propose a web interface that allows nurses to create, modify and delete any medication order. All changes made on the website should instantly flow to mobile for med passes. All med passes captured on mobile should instantly flow to web for reporting.

## Business Intelligence Requirements

### Real-Time Dashboards

We propose a solution that will be entirely cloud and mobile focused so as to ensure real-time, centralized information. For example: the web application will offer frontline staff with visual and audible alerts about their round compliance.

### Gather And Store Data

We will only deploy a solution that leverages a cloud server. This affords staff the ability to instantly compile data from all locations (even across facilities) within 2 seconds, and access logs from any device. The system will create a mobile-friendly set of dashboards so that staff will have instant insights into facility operations from any connected device.

### Compile Reports

We propose a web reporting system that allows supervisors to access any log on the central data repository (cloud hosted). Supervisors will be able to access these reports from any device with internet connectivity, using their unique login credentials. The reporting system will allow for instant querying of logs by: date, time, staff, youth, keyword, workflow module, etc. In addition to these filters, the supervisor will be able to display photos that may have been captured during the mobile logging process.

## Clear Count From Central Dashboard
<span style="float:right">3.8.5</span>

We propose a real-time dashboard that visualizes headcounts. Supervisors will be able to log into the web application, navigate to a Headcount Dashboard and formally initiate a facility-wide headcount. Once initiated, the supervisor can watch the dashboard while officers proceed to account for each and every offender, each scan will update the supervisor's screen in real-time. Once all scans have taken place, the supervisor can formally close the headcount and type justifications for any offender that did not receive a physical scan.

## Flag Supplies
<span style="float:right">3.8.6</span>

We propose a mobile app that logs supply passes. Preferred workflow:

1. Officer scans a wall-mounted RFID tag,

2. Taps the name of one or many offenders,

3. Taps one or more supplies.

This list of supplies will be fully customizable by command staff, including the ability to flag certain items as "requires signature" or "needs to be returned", or "only receives one". These flags will trigger different alerts to the mobile user in that housing unit. Examples of returnable items include: razors, nail clippers, rulebook, tablet, etc.

# Technical Requirements

We agree to comply with all security requirements stipulated by TJJD in this RFO.
<span style="float:right">3.9.1-<br>3.9.13</span>

## Proposed Tech Stack

1. Web App:

    a. SQL Server Reporting Services

    b. ↳ .NET Framework

    c. ↳ SQL Server Database

    d. ↳ Microsoft OS

    e. ↳ AWS Government Cloud

2. Mobile App:

    a. Custom Android Development

The proposed solution will implement user authentication (username/password) that maps to TJJD defined user privileges.

## Legal Considerations

HIPAA - we comply with physical, administrative and security aspects of HIPAA. Examples include but are not limited to:

- Access control - centrally-controlled unique username and PIN code for each user

- Tools for encryption - encrypted sync service to and from server

- Facility access controls - best practices of enterprise cloud provider

- Restricting third-party access - no access by third party organizations

CJIS – Cooper and GUARDIAN RFID require its in-house DBAs to undergo CJIS training prior to database build/access.

FERPA – Cooper and GUARDIAN RFID do not foresee the need for FERPA compliance throughout this particular deployment.

# Section 3 – Deliverables

*The Vendor shall provide a narrative on their approach to completing all of the deliverables as described in this RFO and any additional deliverables the Vendor intends to deliver as part of this project.*

We agree to the requirements stipulated in this RFO regarding Section 3 "Deliverables". We propose the following deliverables in order to create TJJD's Offender Monitoring and Tracking System.

# Our Terminology

**User Story** - Description of the feature requirements, includes the Acceptance Criteria, Assumptions, Tasks needed to build the feature within the system.

**Requirements Complete** - Agreement and sign-off by a correctional officer that user story accurately captures expected results for a feature to be delivered.

**Scope Check** - User Stories must be signed off on by a correctional officer before development can begin. This assures the team we are in alignment on the details of the feature.

**LOW** - Level of Work, the amount of time estimated to complete the task.

**Sprint** - Bound amount of work. Sprints are executed such that entire features can be developed and tested within the sprint. When sprints are completed, any changes or fixes to features which are not Feature Accepted are pushed to later sprints.

**Feature Acceptance** - Agreement and sign-off by a correctional officer that the feature was delivered according to the Acceptance Criteria in the user story

**DevOps** - Identifying and documenting the steps, tools, and procedures to move from one environment to another.

**Check-ins** - Random user testing to verify builds or deployments are successful. Typically used to identify missed steps in deployment and is not intended to be full feature re-testing.

# Our Approach

We will follow a Hybrid Agile implementation methodology for delivering inmate tracking solutions. Hybrid Agile blends the best of Iterative and Predictive approaches with specific checkpoints to ensure ongoing alignment with the correctional agency.

Requirements will be organized into development Sprints that will run concurrently with other project activities such as discovery sessions and quality assurance testing.

During the development phase, the team will interact directly with TJJD correctional officers and project managers in order to define design and development standards as well as iteratively review, elicit feedback and finalize the technology stack with key stakeholders.

Outputs of each development sprint will include comprehensive deliverables including but not limited to:
  • Sprint testing guidelines (review of QA progress to sprint),
  • Expanded prototypes (demonstrations),
  • Project management status reports (weekly),
  • Updated project schedule if needed.
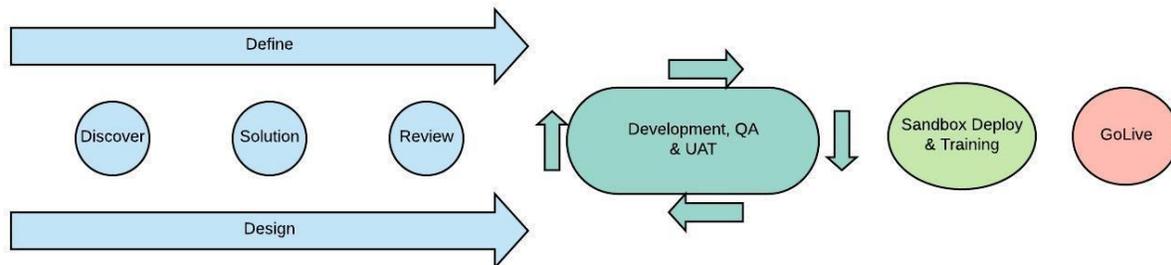


## Our Phases

### Define, Design & Review

During Define & Design Phases, Business Analysts and Solution Architects will work on detailing the scope and architecture of the solution.

Daily Activities will include:
  ● Discovery meetings with correctional officers and wireless internet administrators in order to review user stories, clarify scope and parameters, and document assumptions and details for development & QA teams.

  ● Plan and document future state system architecture

  ● Begin designing UX and UI for features requiring custom interface.

Exit Criteria:
  ● Requirements Complete is required on user stories to assign them to sprints and begin development

Phase Deliverables:
  ● Entity Relationship Diagram (ERD)

- Description of data elements as well as relationships.

- Field level security, profile permissions across objects

- Page wireframes

- Integration Architecture Detailed Design Documentation

## Develop & Review

Phase Deliverables:
- Developing feature as documented (Dev)

- Writing & executing QA test cases on sprint features (QA)

- Demo to customer with request for Feature Acceptance (UAT)

- Requests for clarifications or reviews as necessary

Exit Criteria:
- Agreement and sign-off by a correctional officer that the feature was delivered according to the Acceptance Criteria in the user story

Activities:
- Development is divided into 2-week Sprints. At the end of each sprint is a demonstration and Feature Acceptance by correctional officers at TJJD. UAT plan updates - are to be created during the design & define phase, however these will be reviewed and potentially changed during each sprint. The UAT phase will include Logging & fixing of issues as well as backlogging enhancements for future sprints.

## Sandbox Deploy

Deployment Phase is the work to prepare and launch the solution into TJJD's sandbox environment.

Daily Activities include:
- Preparing a list of deployment, owners, dependencies.

- Gathering manifest items & writing deployment scripts

- Verifying integration updates/changes

- Executing a dry run into a staging environment.

- Check-ins post deployment

Exit Criteria:
- Solution is accessible by administrators in the sandbox environment

## Admin Training

The Admin Training is TJJD's opportunity to run documentation scenarios between mobile and web. All interfaces will be connected to the pre-production system so that administrators (wardens, supervisors, frontline supervisors) can use the sandbox environment, give feedback, and tailor their production parameters and permissions.

Weekly Activities include:
● Supervisors work with GUARDIAN RFID project manager to receive hands-on training in reports, user creation, and Hard Tag settings.

Exit Criteria:
● Agreement and sign-off by a correctional officer that sandbox captures expected results for overall system requirements.

## User Training

Training Guide
● Prior to scheduling any user training, GUARDIAN RFID will create a thorough, written training manual that explains each and every feature within the system. This guide will be printed and shipped to each TJJD facility (one copy for each officer).

Support Troubleshooting Guide
● Prior to scheduling any user training, GUARDIAN RFID will create a support troubleshooting guide for technical staff at TJJD. This guide will focus on Wi-Fi connectivity but also give end-user tips on debugging issues under certain circumstances.

Onsite Training
● A member of the GUARDIAN RFID team will travel onsite to TJJD facilities to give in-person training to all TJJD staff. GUARDIAN RFID does not support train-the-trainer arrangements. Training will take place through 4-hour classes (30-40 officers at a time) and will be immediately followed by on-shift shadowing. GUARDIAN RFID does not support one-off trainings for individual staff members, but instead groups training sessions in classes of 30-40 officers.

Online Training
● GUARDIAN RFID will create training videos for each feature so that TJJD staff may receive ongoing training through a web-based platform.

## Platform Deliverables

● **Web Application** a Cloud-based reporting, integration, and end user management platform that equips supervisors with real-time and historical insights about daily floor operations, offenders, and staff members.

- ○ **Compliance Monitor** a feature within the web app that ensures staff accountability by measuring security round compliance in real-time. Customizable warnings, notifications, and digital clocks help to communicate security round performance.

- ○ **Activity Log** a feature within the web app that gathers floor activities from across the facility and centralizes them into one single information feed.

- ○ **Historic Reports** a feature within the web app that generates electronic reports that can be filtered by offender name, activity type, and more.

- ○ **Incident Workflow** a feature within the web app that carries each step of the due process about incidents, from evidence gathering to hearings, through appeals.

- ○ **Headcount Dashboard** a feature within the web app that establishes a body of evidence for each formal count, while visualizing scans in real-time.

- ○ **Control Panel** a feature within the web app that locates out-of-cell offenders during scheduled activities, and flags offenders with returnable supplies.

- ○ **Operational Intelligence** a feature within the web app, a vantage point from which command staff can clarify threats and predict behaviors.

- ● **Mobile Device/App** a rugged, Android-based solution.

  - ○ **Security Check** a feature within the mobile app that proves the physical presence of officers at each significant step of their security round.

  - ○ **Shake-Down** a feature within the mobile app that builds evidence on items that are illicitly acquired or shared by offenders. Subsequent features include:

    - ■ **Voice-To-Text** - transcribes what officers are saying during shake-downs;

    - ■ **Incident Codes** - present touch-screen phrases to describe the violation;

    - ■ **Photo Capture** - equips staff with an HD camera with Wi-Fi upload.

  - ○ **Face-To-Face** a feature within the mobile app that defends the facility's ordinance of in-person interactions between staff and offenders. Subsequent features include:

    - ■ **Voice-To-Text** - transcribes what officers are saying;

    - ■ **Predefined Observations** - allows staff to tap on canned observations;

- ■ **Voice Translate** - instantly translates what foreign offenders are saying.

  ○ **Out-Of-Cell** a feature within the mobile app that creates an unbreakable chain of movement history on any offender - from booking to release.

  ○ **Meals & Recreation** features within the mobile app that track the acceptance and refusal of meals or recreation. Subsequent features include:

    ■ **Custom Workflow** - customize for any other statutorily required activity.

  ○ **Headcount** a feature within the mobile app that mobilizes line staff to physically scan on every offender, sending a continuous feed of updates to the supervisor.

  ○ **Medication Pass** a feature within the mobile app that documents medication pass, transmitting to OnDemand for eMAR reports. Subsequent features include:

    ■ **Signature Capture** - allows staff to capture touch-screen signatures;

    ■ **Voice-To-Text** - transcribes what officers are saying during med passes;

    ■ **Med Authentication** - allows staff to scan bottles and blister packs;

    ■ **Photo Capture** - equips staff with an HD camera with Wi-Fi upload;

    ■ **Video Capture** - equips staff with an HD video camera with Wi-Fi upload.

  ○ **Clock App** an app standard to the Android OS that allows staff to create custom reminders with distinct names and ringtones.

  ○ **Incident Workflow** a feature within the mobile app that tracks due process for incidenting, from initial evidence capture through the hearings process.

  ○ **Asset Tracker** a feature within the mobile app that reminds staff to track the condition and depletion or high-cost assets throughout the facility.

- ● **Wall-Mounted RFID Tags** multifunctional sensors that can automate security checks and cell checks, offender movements, offender activity logging, and more.

Cooper Consulting

# Section 4 – Project Management Plan

*The Vendor shall provide an initial project management plan that includes all areas specified in Section this RFO. The Vendor shall also identify all exceptions it takes to the technical requirements of the solicitation and all deviations for which it requests approval.*

*NO PRICING DATA SHALL BE SUBMITTED IN THIS TAB.*

We agree to the requirements stipulated in this RFO regarding Section 4 "Project Management Plan" We propose the following Project Work Plan in order to create TJJD's Offender Monitoring and Tracking System.

| Deliverable No. | Sprint Description | Agency Requirements | 2 Week Sprint |
|---|---|---|---|
| 0 | High-level Define & Design | Availability for discovery | 1 |
| 0 | High-level Define & Design | Availability for discovery | 2 |
| 0 | High-level Define & Design | Availability for discovery | 3 |
| 1 | Hardware Provisioning | Installation plan for each facility | 4 |
| 2 | "Import" API | Dedicated API expert | 5 |
| 3 | Security Check (mobile) | Availability for UAT | 6 |
| 3 | Shake-Down (mobile) | Availability for UAT | 7 |
| 3 | Face-To-Face (mobile) | Availability for UAT | 8 |
| 3 | Out-Of-Cell (mobile) | Availability for UAT | 9 |
| 3 | Headcount (mobile) | Availability for UAT | 10 |
| 3 | Medication Pass (mobile) | Availability for UAT | 11 |
| 3 | Incident Workflow (mobile) | Availability for UAT | 12 |
| 3 | Asset Tracker (mobile) | Availability for UAT | 13 |
| 4 | Admin Training (mobile) | Sandbox Sign-Off | 14 |
| 5 | Compliance Monitor (web) | Availability for UAT | 15 |
| 5 | Activity Log (web) | Availability for UAT | 16 |
| 5 | Incident Workflow (web) | Availability for UAT | 17 |
| 5 | Headcount Dashboard (web) | Availability for UAT | 18 |
| 5 | Control Panel (web) | Availability for UAT | 19 |
| 5 | Historic Reports (web) | Availability for UAT | 20 |
| 5 | Operational Intelligence (web) | Availability for UAT | 21 |

| Deliverable No. | Sprint Description | Agency Requirements | 2 Week Sprint |
|---|---|---|---|
| 6 | Admin Training (web) | Sandbox Sign-Off | 22 |
| 7 | "Export" API | Dedicated API expert | 23 |
| 8 | Training Guide | Availability for review and approval | 24 |
| 9 | User Training | Availability for onsite training (all staff) | 25 |
| 10 | Go-Live Support | Dedicated support contact | 26 |
| 11 | Post Go-Live Support | n/a | n/a |
| 12 | SaaS Platform Upkeep | n/a | n/a |

# FINAL EXHIBIT B - PRICE FORM V3
# BAFO

**Proposal of:** Cooper Consulting Company

_____

(Respondent Company Name)

**Ref.:** Offender Monitoring and Tracking System
**RFO No.:** 644-9-070319

Having carefully examined all the specifications and requirements of this Request for Offer (RFO) and any attachments thereto, the Respondent proposes to furnish the software and technical services required pursuant to this RFO.

**<u>The Agency reserves the option to acquire all or portions of the product and services.</u>**

**Pricing for Services Offered** (notate appropriately whether cost(s) are one-time or ongoing)

| Service | Quantity/ Labor Hours | Cost/Rate | Total Cost | One-time or Ongoing |
|---|---|---|---|---|
| **Testing and User Acceptance \*\*\*\*** | 90 hours | $330.00 | $29,700.00 | One-time |
| **System Administration Knowledge Transfer** | 23 hours | $430.43 | $9899.89 | One-time |
| **Implementation Plan** | 46 hours | $275.00 | $12,650.00 | One-time |
| **Training Program and Plan \*\*\*** | 22 days | $1,644.50 | $36,179.00 | One-time |
| **Maintenance and Support** | 45 hours | $220.00 | $9,900.00 | One-time |
| **Services** | - | - | - | - |
| **-- Enhancements** | unknown | $550 / hr | unknown | n/a |
| **-- Change Requests** | unknown | $550 / hr | unknown | n/a |
| **RFID Hard Tags Quantity: 1,400** | 1400 units | $16.45 | $ 23,030.00 | One-time |
| **Android Devices Quantity: 107** | - | - | - | - |
| **-- Owned** | 107 units | $2,524.50 | $270,121.50 | One-time |
| **-- Leased** | 107 units | $990.00 | $105,930.00 | Ongoing |
| **Product Support \*\*\*\*\*** | 107 units | $495.00 | $ 52,965.00 | Ongoing |
| **\*\*Maintenance** | Full year | $11,000.00 | $11,000.00 | Ongoing |
| **\*Additional Required Services, if applicable (must specify the service)** | n/a | n/a | n/a | n/a |
| **Grand Total Cost** | - | - | - | - |
| **-- Owned, One-time** | | | $444,445.39 | |

| | | | |
|---|---|---|---|
| -- Owned, Ongoing | | $63,965.00 | |
| -- Leased, One-time | | $280,467.00 | |
| -- Leased, Ongoing | | $169,895.00 | |

*Additional Required Services – Vendor identified services that are required in order for the Vendor to provide their proposed solution that do not fall under the cost categories listed.

**Cooper will offer the first year of support as a complementary service. Yearly payment will be due on the anniversary of the first facility's go-live.

*** Initially, GUARDIAN RFID proposed 30 days of training, assuming that there would be 30 officers per class (+ 4 days as additional padding). During the BAFO stage, GUARDIAN RFID proposed 22 days of training, assuming that there could be as many as 40 officers per class (+ 1 day as additional padding). Please see the following assumptions from the GUARDIAN RFID pre-sales team:

| Facility | Pods Per Facility* | Officers Per Facility** | Training Days (40 officers per class) | Training Days (30 officers per class) |
|---|---|---|---|---|
| Evins Regional Juvenile Center | 10 | 70 | 2 | 3 |
| Gainesville State School | 12 | 84 | 3 | 3 |
| Giddings State School | 16 | 112 | 3 | 4 |
| McLennan County State | 22 | 154 | 4 | 6 |
| Ron Jackson State Juvenile | 14 | 98 | 3 | 4 |
| Ayers House | 1 | 7 | 1 | 1 |
| Brownwood Halfway House | 1 | 7 | 1 | 1 |
| Edna Tamayo House | 1 | 7 | 1 | 1 |
| McFadden Ranch | 2 | 14 | 1 | 1 |
| Schaeffer House | 1 | 7 | 1 | 1 |
| Willoughby House | 1 | 7 | 1 | 1 |
| Sub Total | | | 21 | 26 |
| Padding | | | 1 | 4 |
| **Grand Total** | | | **22** | **30** |

*Numbers taken from RFO- 644-9-070319-OMTS.

**Numbers assumed by GUARDIAN RFID pre-sales team.

**** This was not an additional charge, but rather a reallocating of services from Testing and User Acceptance to Maintenance and Support (39,600 - 29,700 = 9,900). GUARDIAN RFID took advantage of the BAFO stage to reallocate these services due to discussions that took place after the initial submittal. Our team feels that this project may in fact demand more go-live support than quality assurance, given the fact that it entails 11 separate facilities.

***** The price per device increased due to the reduction of 80 devices. Our supplier charges lower cost per unit for higher quantities and higher cost per unit for smaller quantities. (Originally reported this as a typo – it was not.)

<u>**EXHIBIT C**</u>
<u>**TJJD'S CERTIFICATIONS AND GENERAL PROVISIONS**</u>


**IF ANY OF THE TERMS AND CONDITIONS IN THE CERTIFICATIONS AND GENERAL PROVISIONS SECTIONS BELOW, SECTIONS I AND II, RESPECTIVELY, CONFLICT WITH ANY OF THE TERMS AND CONDITIONS OF SERVICE PROVIDER'S CONTRACT WITH DIR, THE TERMS AND CONDITIONS OF SERVICE PROVIDER'S DIR CONTRACT TAKE PRECEDENCE.**

**I. CERTIFICATIONS**

**Article 1: Equal Opportunity**

Service Provider certifies compliance with all terms, provisions, and requirements of Titles VI and VII, Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, and any other federal, state, local, or other anti-discriminatory act, law, statute, or regulation, along with all amendments and revisions of the acts, laws, statutes, or regulations, in the performance of this contract, and will not discriminate against any child or youth, client, employee, or applicant for employment because of race, creed, religion, age, sex, color, national or ethnic origin, handicap, or any other illegal discriminatory basis or criteria.

**Article 2: Unfair Business Practices**

Service Provider certifies that neither it nor its officers have been found guilty in a judicial or state administrative agency proceeding of unfair business practices as set out in the Texas Business and Commerce Code and that no officer of Service Provider has served as an officer of another company which has been found guilty in a judicial or state administrative agency proceeding of unfair business practices. If the above certifications are false, the contract is void.

**Article 3: Franchise Taxes**

**Section 1**: Service Provider certifies that should Service Provider be subject to payment of Texas franchise taxes, all franchise taxes are current. If such certification is false, the contract may be terminated at the option of TJJD or other administrative error sanctions may be taken.
**Section 2:** If Service Provider is exempt from payment of Texas franchise taxes, Service Provider shall so indicate by attachment to the contract.
**Section 3**: If Service Provider's payment of Texas franchise taxes becomes delinquent during the term of the contract, Service Provider will notify TJJD within 24 hours. If such delinquency cannot be cured within 24 hours and a copy of the Certification of Account Status proving payment of delinquent taxes cannot be provided to TJJD, the contract may be terminated at the option of TJJD or other administrative error sanctions may be taken under the provisions of the contract.

**Article 4: Required Disclosure of Lobbyist Activity and Certificate of Interested Parties**

Service Provider agrees that if, at any time during the term of the contract, an employee, director, subconsultant, or subcontractor of Service Provider is required to register as a lobbyist under Texas Government Code Chapter 305, Service Provider shall notify TJJD and provide timely copies of all reports filed with the Texas Ethics Commission, as required by Chapter 305.

Additionally, pursuant to House Bill 1295 and Texas Government Code Section 2252.908, Service Provider must submit a Certificate of Interested Parties or disclosure of interested parties on a form prescribed by the Texas Ethics Commission, currently identified as Form 1295. Prior to submission of this signed contract to TJJD, Service Provider must file Form 1295 through the online filing application process on the Texas Ethics Commission website at https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm. TJJD will acknowledge Service Provider's Form 1295 within thirty (30) days of submission.

## Article 5: Notification to TJJD of Subconsultants and Subcontractors

**Section 1:** Service Provider shall notify TJJD of the selection and/or use of all subcontractors or subconsultants regularly used by Service Provider in performing or assessing the performance of Service Provider's duties under the contract if paid or anticipated to be paid an amount exceeding five thousand dollars ($5,000.00) during the term of the contract. Service Provider may not use subcontractors and subconsultants to perform Service Provider's duties under the contract without prior written approval of TJJD. Approval will not be unreasonably withheld.

**Section 2:** No contractual relationship will exist between Service Provider's subconsultants or subcontractors and TJJD. TJJD shall have no responsibility whatsoever for the conduct, actions, or commissions (active or passive) of any subconsultants or subcontractors in the performance of their duties under the contract.

**Section 3:** Service Provider shall be solely responsible for the management of any subconsultants or subcontractors in the performance of their duties under this contract.

## Article 6: Compliance with Child Support, Section 231.006, Texas Family Code

**Under Section 231.006, Family Code, the vendor or applicant [Service Provider] certifies that the individual or business entity named in this contract, bid, or application is not ineligible to receive the specified grant, loan, or payment and acknowledges that this contract may be terminated and payment may be withheld if this certification is inaccurate.** A bid or an application for a contract, grant, or loan paid from state funds must include the name and social security number of the individual or sole proprietor and each partner, shareholder, or owner with an ownership interest of at least 25 percent of the business entity submitting the bid or application.

SERVICE PROVIDER MUST PROVIDE, IN THE SPACE BELOW, THE NAME AND SOCIAL SECURITY NUMBER OF AN INDIVIDUAL OWNER, A SOLE PROPRIETOR, AND ALL PARTNERS, SHAREHOLDERS, OR OWNERS WITH AN OWNERSHIP INTEREST OF AT LEAST TWENTY-FIVE (25) PERCENT OF THE BUSINESS ENTITY ENTERING INTO THE CONTRACT.

For business entities with no identifiable owner of twenty-five percent (25%) or more of the entity, indicate with "NONE" on the first line below.

| Name: | Social Security Number: |
|-------|------------------------|
| Melynda B. Caudle | ███████ |

**FEDERAL PRIVACY ACT NOTICE:** This notice is given pursuant to the Federal Privacy Act. Disclosure of your Social Security Number (SSN) is required under Section 231.006(c) and Section 231.302(c)(2) of the Texas Family Code. The SSN will be used to identity persons that may owe child support. The SSN will be kept confidential to the fullest extent allowed under Section 231.302(e), Texas Family Code.

**Article 7: Compliance with Section 572.054, Texas Government Code, Former Officer or Employee of TJJD**

Service Provider certifies compliance with Texas Government Code Section 572.054. Service Provider has not employed a former officer or employee of TJJD to perform services on Service Provider's behalf, to secure the contract, or to represent Service Provider in any manner prohibited by Section 572.054. A false certification could result in termination of the contract, withholding of payments, or other administrative error sanctions.

**Article 8: Compliance with Section 2252.901, Texas Government Code, Former or Retired Employee of the Agency**

Service Provider represents and warrants that none of its employees including, but not limited to, those authorized to provide services under the contract, were former employees of TJJD during the twelve (12) month period immediately prior to the date of execution of the contract.

This requirement applies to employment contracts and professional services and consulting services contracts under Texas Government Code Chapter 2254 with former or retired TJJD employees, as indicated by Texas Government Code Section 2252.901, which reads, "A state agency may not enter into an employment contract, a professional services contract under Chapter 2254, or a consulting services contract under Chapter 2254 with a former or retired employee of the agency before the first anniversary of the last date on which the individual was employed by the agency, if appropriated money will be used to make payments under the contract. This section does not prohibit an agency from entering into a professional services contract with a corporation, firm, or other business entity that employs a former or retired employee of the agency within one year of the employee's leaving the agency, provided that the former or retired employee does not perform services on projects for the corporation, firm or other business entity that the employee worked on while employed by the agency."

**Article 9: Suspension and Debarment**

Service Provider 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. Entities ineligible for federal procurement are listed at http://www.sam.gov.

**Article 10: Excluded Parties/Terrorism**

Service Provider certifies that it is not listed in the prohibited vendors list authorized by Executive Order No. 13224, *"Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism",* published by the United States Department of the Treasury, Office of Foreign Assets Control.

**Article 11: Prior Disaster Relief Contract Violation**

**Under Section 2155.006 and 2261.053, Government Code, the vendor [Service Provider] 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.**

A state agency may not accept a bid or award a contract, including a contract for which purchasing authority is delegated to a state agency, that includes proposed financial participation by a person who, during the five-year period preceding the date of the bid or award, has been: (1) convicted of violating a federal law in connection with a contract awarded by the federal government for relief, recovery, or reconstruction efforts as a result of Hurricane Rita, as defined by Section 39.459, Utilities Code, Hurricane Katrina, or any other disaster occurring after September 24, 2005; or (2) assessed a penalty in a federal civil or administrative enforcement action in connection with a contract awarded by the federal government for relief, recovery, or reconstruction efforts as a result of Hurricane Rita, as defined by Section 39.459, Utilities Code, Hurricane Katrina, or any other disaster occurring after September 24, 2005.

**Article 12: Antitrust**

Service Provider represents and warrants that, in accordance with Section 2155.005 of the Texas Government Code, neither Service Provider nor the firm, corporation, partnership, or institution represented by Service Provider, or anyone acting for such a firm, corporation or institution has (1) violated any provision of the Texas Free Enterprise and Antitrust Act of 1983, Chapter 15 of the Texas Business and Commerce Code, or the federal antitrust laws, or (2) communicated directly or indirectly the contents of this contract to any competitor or any other person engaged in the same line of business as Service Provider.

**Article 13: Intellectual Property Indemnification**

SERVICE PROVIDER SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS TJJD AND THE STATE OF TEXAS FROM AND AGAINST ANY AND ALL CLAIMS, VIOLATIONS, MISAPPROPRIATIONS OR INFRINGEMENT OF ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHTS AND/OR OTHER INTANGIBLE PROPERTY, PUBLICITY OR PRIVACY RIGHTS, AND/OR IN CONNECTION WITH OR ARISING FROM: (1) THE PERFORMANCE OR ACTIONS OF SERVICE PROVIDER PURSUANT TO THIS CONTRACT; (2) ANY DELIVERABLE, WORK PRODUCT, CONFIGURED SERVICE OR OTHER SERVICE PROVIDED HEREUNDER; AND/OR (3) TJJD'S AND/OR SERVICE PROVIDER'S USE OF OR ACQUISITION OF ANY REQUESTED SERVICES OR OTHER ITEMS PROVIDED TO TJJD BY SERVICE PROVIDER OR OTHERWISE TO WHICH TJJD HAS ACCESS AS A RESULT OF SERVICE PROVIDER'S PERFORMANCE UNDER THE CONTRACT. SERVICE PROVIDER AND TJJD AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM. SERVICE PROVIDER SHALL BE LIABLE TO PAY ALL COSTS OF DEFENSE, INCLUDING ATTORNEYS' FEES. THE DEFENSE SHALL BE COORDINATED BY SERVICE PROVIDER WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL (OAG) WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND SERVICE PROVIDER MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM OAG. IN ADDITION, SERVICE PROVIDER WILL REIMBURSE TJJD AND THE STATE OF TEXAS FOR ANY CLAIMS, DAMAGES, COSTS, EXPENSES OR OTHER AMOUNTS, INCLUDING, BUT NOT LIMITED TO, ATTORNEYS' FEES AND COURT COSTS, ARISING FROM ANY SUCH CLAIM. IF TJJD DETERMINES THAT A CONFLICT EXISTS BETWEEN ITS INTERESTS AND THOSE OF SERVICE PROVIDER OR IF TJJD IS REQUIRED BY APPLICABLE LAW TO SELECT SEPARATE COUNSEL, TJJD WILL BE PERMITTED TO SELECT SEPARATE COUNSEL AND SERVICE PROVIDER WILL PAY ALL REASONABLE COSTS OF TJJD'S COUNSEL.

**Article 14: Contracting with Executive Head of State Agency**

In accordance with Section 669.003 of the Texas Government Code, relating to contracting with the executive head of a state agency, Service Provider certifies that it is not (1) the executive head of TJJD, (2) a person who at any time during the four years before the date of the contract was the executive head of TJJD, or (3) a person who employs a current or former executive head of TJJD. Or Service Provider and TJJD have complied with the requirements of Section 669.003 concerning board approval and notice to the Legislative Budget Board.

**Article 15: Abandonment or Default**

If Service Provider defaults on the contract, TJJD reserves the right to cancel the contract without notice and either resolicit bids or award the contract to the next best responsive and responsible Service Provider. The defaulting Service Provider will not be considered in the resolicitation and may not be considered in future solicitations for the same type of work, unless the specifications or scope of work are significantly different. The period of suspension will be determined by TJJD based on the seriousness of the default.

**Article 16: Certain Bids and Contracts Prohibited**

Under Texas Government Code, Section 2155.004, TJJD may not accept a bid or award a contract that includes proposed financial participation by a person who received compensation from TJJD to participate in preparing the specifications or request for proposals on which the bid or contract is based. If Service Provider is not eligible, then the contract may be immediately terminated. **Under Section 2155.004, Government Code, the vendor [Service Provider] certifies that the individual or business entity named in this bid or contract is not ineligible to receive the specified contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate.**

**Article 17: Gifts and Gratuity**

Pursuant to Section 2155.003 of the Texas Government Code, Service Provider represents and warrants that it has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with the contract.

**Article 18: False Statements and Conflict of Interest:**

All statements and information prepared and submitted in the contract is current, complete, and accurate; Service Provider has disclosed in writing to TJJD all existing or potential conflicts of interest relative to the performance of the contract; and if circumstances change during the course of the contract, Service Provider shall promptly notify TJJD.

**Article 19: Access to Information**

Information, documentation, and other material in connection with this solicitation or any resulting contract may be subject to public disclosure pursuant to Chapter 552 of the Texas Government Code (the "Public Information Act"). In accordance with Section 2252.907 of the Texas Government Code, Service Provider is required to make any information created or exchanged with the State pursuant to the contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State. Such formats include, but are not necessarily limited to, in a non-encrypted electronic format, PDF, and HTML.

**Article 20: Verification of Worker Eligibility Clause**

Service Provider certifies that for contracts for services, Service Provider shall utilize the U.S. Department of Homeland Security's E-Verify system (E-Verify) during the term of the contract to determine the eligibility of:
1. all persons employed by Service Provider to perform duties within Texas; and
2. all persons, including subcontractors, assigned by Service Provider to perform work

pursuant the contract within the United States of America.

Service Provider shall provide, upon written request by TJJD, an electronic or hard copy screenshot of the confirmation that Service Provider is enrolled in E-Verify. Service Provider shall provide, upon written request by TJJD, an electronic or hard copy of the confirmation or non-confirmation screen containing the E-Verify case verification number for attachment to the Form I-9 for each Service Provider employee, subcontractor, and subcontractor employee that meet the criteria above, following any required E-Verify protocols to allow for the provision of such information.

If it is determined that Service Provider has violated the certifications set forth in this Article, then (1) Service Provider shall be in breach of contract, (2) TJJD shall have the option to terminate the contract for cause without prior notice, and (3) in addition to any other rights or remedies available to TJJD under the contract, Service Provider shall be responsible for all costs incurred by TJJD to obtain substitute services to replace the terminated contract.

**Article 21: Prohibition on Contracts with Companies Boycotting Israel**

Pursuant to Section 2270.002 of the Texas Government Code, Service Provider certifies that either: (i) it meets an exemption criterion under Section 2270.002; or (ii) that it does not, and shall not for the duration of the contract, boycott Israel as the term is defined by 808.001(1) of the Texas Government Code.

**Article 22: Prohibition on Contracts with Companies Engaged in Business with Iran, Sudan, or Foreign Terrorist Organizations**

Section 2252.152 of the Texas Government Code prohibits TJJD from awarding a contract to any person who does business with Iran, Sudan, or a foreign terrorist organization as defined in Section 2252.151 of the Texas Government Code. Service Provider certifies that it is not ineligible to receive the contract.

**Article 23: Disaster Recovery Plan**

Upon request of TJJD, Service Provider shall provide copies of its most recent business continuity and disaster recovery plans.

**Article 24: Cybersecurity Training**

If Service Provider, including subcontractor, officer, or employee of Service Provider, has access to a state computer system or database, then Service Provider and any applicable subcontractor, officer, or employee of Service Provider, must complete a cybersecurity training program (Program) certified under Texas Government Code Section 2054.519 as selected by TJJD. The

Program must be completed during the term of the contract and during any renewal period thereafter, if applicable.

## II. GENERAL PROVISIONS

**Article 1: Relationship of Parties**

Service Provider is acting as an independent contractor and is wholly responsible for the day-to-day operations of its programs and employees. No joint venture, partnership, or agency exists, nor shall be implied by the terms of the contract. No employee of Service Provider shall become an employee of TJJD by virtue of the contract.

Service Provider agrees and acknowledges that during the existence of the contract, Service Provider shall be entirely responsible for the liability and payment of Service Provider's and Service Provider's employees' taxes of whatever kind, arising out of the performance of the contract. Service Provider agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and workers' compensation. TJJD shall not be liable to Service Provider, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or workers' compensation or any benefit available to a TJJD or other state employee. Further, Service Provider shall indemnify and hold harmless TJJD, state agencies, the State of Texas, and/or their employees, agents, representatives, and/or assignees from any liability, actions, claims, demands, or suits, and all related costs, attorneys' fees, and expenses relating to tax liability, unemployment insurance, and/or workers' compensation payments.

**Article 2: Indemnity**

**SERVICE PROVIDER SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS THE STATE OF TEXAS AND TJJD, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, AND/OR DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF, OR RESULTING FROM ANY ACTS OR OMISSIONS OF SERVICE PROVIDER OR ITS AGENTS, EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR PERFORMANCE OF THE CONTRACT AND ANY PURCHASE ORDERS ISSUED UNDER THE CONTRACT. THE DEFENSE SHALL BE COORDINATED BY SERVICE PROVIDER WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND SERVICE PROVIDER MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM THE OFFICE OF THE TEXAS ATTORNEY GENERAL. SERVICE PROVIDER AND TJJD AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM.**

**Article 3: Proof of Financial Stability and Financial Reporting**

If TJJD has credible information that calls into question Service Provider's ability to meet its financial obligations, TJJD may require Service Provider to provide proof of financial stability.

Correspondence from Service Provider's independent auditor that Service Provider is able to meet its current financial commitments shall suffice as proof of financial stability.

Service Provider shall provide an itemized cost breakdown in conjunction with invoices to indicate how TJJD/State of Texas funds are being used to provide services during the contract term.

### Article 4: Liability Insurance

**Section 1:** Service Provider shall maintain liability insurance in the amount of $1,000,000.00 per occurrence with a separate aggregate limit of $2,000,000.
**Section 2:** Service Provider shall provide proof of insurance documents to TJJD Contracts Department, upon request.
**Section 3:** The required insurance coverage, in the above stated amount, must be maintained during the term of the contract and through any subsequent extensions. Failure to maintain the required insurance coverage may result in termination of the contract or administrative error sanctions.

### Article 5: Confidentiality and Security

Service Provider agrees that all of its employees, contractors, subcontractors, and associates will maintain the confidentiality of all juvenile records and identifying information.

Service Provider and all of its employees, contractors, subcontractors, and associates performing maintenance, development, and/or system or database administration must complete the requisite fingerprint and background checks before being authorized to perform work under the contract.

### Article 6: Administrative Error Sanctions

**Section 1:** In addition to its authority to terminate the contract under Article 7 below or other provisions of the contract, TJJD, based on information from monitoring or other verifiable sources, may take other actions including, but not limited to:
a.  Requiring Service Provider to take specific corrective actions in order to remain in compliance with the terms of the contract; and/or
b.  Recouping payment made to Service Provider; and/or
c.  Imposing recommendations from audit or investigative findings, and minor or major sanctions; and/or
d.  Assessing liquidated damages to the extent allowed by Texas law for each instance of non-compliance; and/or
e.  Suspending, placing into abeyance, or removing any contractual rights including, but not limited to, withholding payment.

**Section 2**: Service Provider shall cooperate fully with TJJD and its authorized representatives in carrying out corrective action plans.

**Article 7: Termination**

**Section 1:** Service Provider may terminate, for convenience, its obligations under the contract by giving thirty (30) days' written notice to TJJD.

**Section 2:** TJJD may terminate, for convenience, its obligations under the contract by giving thirty (30) days' written notice to Service Provider.

**Section 3:** TJJD shall terminate the contract in the event that TJJD is not granted funding to pay for the herein described services or in the event that funding is lost due to either a reduction in the budget or a reallocation of budgeted funds.

**Section 4:** Cause/Default/Breach: If Service Provider fails to provide the goods or services contracted for according to the provisions of the contract or fails to comply with any terms or conditions of the contract, TJJD may, upon written notice of default or breach to Service Provider, immediately terminate all or any part of the contract. Termination is not an exclusive remedy, but exists in addition to any other rights and remedies provided in equity, by law, or under the contract. TJJD may exercise any other right, remedy, or privilege available to it under applicable law or may proceed by appropriate court action to enforce the provisions of the contract. The exercise of any of the foregoing remedies will not constitute a termination of the contract unless TJJD notifies Service Provider in writing prior to the exercise of such remedy. Service Provider shall be liable for all costs and expenses, including court costs, incurred by TJJD with respect to the enforcement of any of the remedies listed herein.

**Section 5:** Termination of the contract shall not release Service Provider from liability or obligation set forth in the contract that is expressly stated to survive termination or by its nature would be intended to be applicable following termination, including, but not limited to, provisions regarding confidentiality, indemnification, transition, records, audit, property rights, dispute resolution, and invoice and fee verifications.

**Article 8: Funding Out Clause**

The contract is subject to termination or cancellation, without penalty to TJJD, either in whole or in part, subject to the availability of state funds. TJJD is a state agency whose authority and appropriations are subject to actions of the Texas Legislature. If TJJD becomes subject to a legislative change, revocation of statutory authority, or lack of appropriated funds that would render either TJJD's or Service Provider's delivery or performance under the contract impossible or unnecessary, the contract will be terminated or cancelled and be deemed null and void. In the event of a termination or cancellation under this Section, TJJD will not be liable to Service Provider for any damages that are caused or associated with such termination or cancellation and TJJD will not be required to give prior notice.

**Article 9: Waiver**

No waiver by either party of any breach or default of the other under the contract shall operate as a waiver of any future or other breach or default, whether of a like or different character or nature.

**Article 10: Severability**

The provisions of the contract are severable. If any provision of the contract is determined by a court of law or other competent authority to be invalid and contrary to any federal, state, or local law, such invalidity shall not affect the other provisions or applications of the contract, which can be given effect without the invalid provision or application.

**Article 11: Contract Term**

See **SECTION I: CONTRACT TERM**

**Article 12: Contract Amendment and Merger Clause**

The contract encompasses the complete and entire agreement of the parties. Neither party has made or relied on any representations, stipulations, or agreements other than those expressly contained in the contract. No other contracts or agreements, oral or written, shall constitute a part of the contract unless such is made in writing, executed by the parties hereto or their successors, and expressly made a part of the contract. The contract may only be amended or supplemented by written amendment, executed by the parties hereto or their successors, and expressly made a part of the contract, except that TJJD reserves the right to make unilateral minor administrative changes to correct typographical errors or change the TJJD contract identification number.

**Article 13: Notice of Changes**

**Section 1:** Service Provider shall notify TJJD immediately in writing in advance of any significant change affecting Service Provider, including, but not limited to, change of Service Provider's name or identity, location of services, ownership or control, operating entity, governing board membership, key personnel, payee identification number, and any other significant changes that may affect the delivery of services under the terms of the contract.
**Section 2:** Service Provider shall not transfer or assign the contract or enter into any subcontract for the services under the contract without prior written approval from TJJD.
**Section 3:** Service Provider shall not relocate the services provided under the contract from the location to be stated in the preamble without prior written approval from TJJD and a certification that the location to which services are to be relocated is in compliance with Chapter 244, Texas Local Government Code, if applicable.

**Article 14: Notice**

*See SECTION IV: NOTICES AND CONTACTS*

**Article 15: Governing Law and Venue**

The contract shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the contract is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to TJJD.

**Article 16: Problem Solving in the Ordinary Course of Business**

**Section 1:** The parties to the contract shall use the procedures contained in this Article for routine problem solving. These procedures may also be used if a party is asserting a claim for breach of contract. Should these procedures not resolve claims for breach of the contract, the procedures contained in Article 17 below shall be followed thereafter.
**Section 2:** Informal Resolution: Service Provider and TJJD staff will communicate regularly and engage in informal problem solving efforts as a routine measure, thus preventing differences from becoming major problems. When routine measures have been exhausted, Service Provider and TJJD staff are encouraged to utilize the following mechanism to resolve problems.
**Section 3:** Formal Resolution:
a. Service Provider or TJJD staff who wish to submit problems for resolution may do so in writing, including all relevant information and a recommended resolution (Statement of Problem).
b. The Statement of Problem will be submitted to the designated contact, unless the problem specifically involves the designated contact, in which case, it will be submitted to the designated contact's supervisor.
c. Problems are to be addressed within ten (10) working days; a written decision will be sent to the individual or program that submitted it, to the designated contact, and to the designated contact's supervisor.
**Section 4:** Appeal: Service Provider or TJJD staff desiring to appeal the decision may do so in writing, within ten (10) working days from the date of written decision, by providing all pertinent information relevant to the appeal to the designated contact's supervisor if the problem was originally addressed by the designated contact, or to the Office of General Counsel if the problem was addressed by the designated contact's supervisor. When appealed, the problem shall be addressed within fourteen (14) working days, with written responses sent to the individual or program who submitted it, the designated contact, the designated contact's supervisor, and the Office of General Counsel.

**Article 17: Claims for Breach of Contract**

The dispute resolution process provided for in Chapter 2260 of the Texas Government Code must be used to attempt to resolve any dispute arising under this contract. If the Service

Provider's claim for breach of contract cannot be resolved informally with TJJD, the claim shall be submitted to the negotiation process provided in Chapter 2260. However, Chapter 2260 does not waive sovereign immunity to suit or liability.

To initiate the process, Service Provider shall submit written notice, as required by Chapter 2260, to the individual identified in the contract for receipt of notices. Any informal resolution efforts shall in no way modify the requirements or toll the timing of the formal written notice of a claim for breach of contract required under Section 2260.051 of the Texas Government Code. Compliance by the Service Provider with Chapter 2260 is a condition precedent to the filing of a contested case proceeding under Chapter 2260.

The contested case process provided in Chapter 2260 is the Service Provider's sole and exclusive process for seeking a remedy for an alleged breach of contract by TJJD, defended by the Office of the Attorney General, if the parties are unable to resolve their disputes as described above. Notwithstanding any other provision of the contract to the contrary, unless otherwise requested or approved in writing by TJJD, the Service Provider shall continue performance and shall not be excused from performance during the period any breach of contract claim or while the dispute is pending. However, the Service Provider may suspend performance during the pendency of such claim or dispute if Service Provider has complied with all provisions of Section 2251.051 of the Texas Government Code (Vendor Remedy for Nonpayment of Contract), and such suspension of performance is expressly applicable and authorized under that law.

**Article 18: No Third Party Beneficiaries**

The terms of the contract are for the sole benefit of the parties to the contract and will not be construed to confer any rights on any other person.

**Article 19: Audit Clause**

Pursuant to Section 2262.154 of the Texas Government Code, the state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under any contract or indirectly through a subcontract under the contract. The acceptance of funds by the Service Provider or any other entity or person directly under the contract or indirectly through a subcontract under the contract acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, the Service Provider or other entity that is the subject of an audit or investigation by the state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit. Service Provider shall ensure that this paragraph concerning the authority to audit funds received indirectly by subcontractors through the contract and the requirement to cooperate is included in any subcontract it awards.

Service Provider shall maintain and retain supporting fiscal documents adequate to ensure that claims for contract funds are in accordance with TJJD and State of Texas requirements. Service Provider shall maintain all such documents and other records relating to this contract and the State's property for a period of seven (7) years after the date of submission of the final invoices or until a resolution of all billing questions or contract issues, whichever is later. Service Provider shall make available at reasonable times and upon reasonable notice, and for reasonable periods, all information related to the State's property, such as work papers, reports, books, data, files, software, records, and other supporting documents pertaining to this contract, for purposes of inspecting, monitoring, auditing, or evaluating by TJJD, the State of Texas, or their authorized representatives. Service Provider shall cooperate with auditors and other authorized TJJD and State of Texas representatives and shall provide them with prompt access to all of such State's property as requested by TJJD or the State of Texas. Service Provider's failure to comply with this Article shall constitute a material breach of this contract and shall authorize the TJJD to immediately assess liquidated damages. TJJD may require, at Service Provider's sole cost and expense, independent audits by a qualified certified public accounting firm of Service Provider's books and records or the State's property. The independent auditor shall provide TJJD with a copy of such audit at the same time it is provided to Service Provider. TJJD retains the right to issue a request for proposals for the services of an independent certified public accounting firm under this contract.

The contract may be amended unilaterally by TJJD to comply with any rules and procedures of the state auditor in the implementation and enforcement of Section 2262.154 of the Texas Government Code.

**Article 20: Debt Owed to State of Texas**

Terms of payment shall be in accordance with Chapter 2251 of the Texas Government Code and in accordance with Section 403.0551 of the Texas Government Code. Any payments owed to Service Provider under the contract will be applied toward elimination of Service Provider's indebtedness to the state or delinquency in payment of taxes to the state until the indebtedness or delinquency is paid in full. Service Provider agrees that any payments due under the contract will be applied towards any debt Service Provider owes to the State of Texas, including, but not limited to, delinquent taxes, delinquent student loan payments, and unpaid child support payments.

**Article 21: Specifications**

Service Provider shall provide services in accordance with the specifications contained in the contract. TJJD will determine the answers to all questions that may arise as to the interpretation of the specifications and the quality or acceptability of work performed. TJJD will decide the rate of progress of the work and the acceptable fulfillment of services on the part of Service Provider.

**Article 22: Assignment**

Without the prior written consent of TJJD, Service Provider may not assign the contract, in whole or in part, or any right or duty required under it.

**Article 23: Compliance with Other Laws**

In the execution of the contract, Service Provider shall comply with all applicable federal, state, and local laws, including laws governing labor, equal employment opportunity, safety, and environmental protection. Service Provider shall make itself familiar with and at all times shall observe and comply with all federal, state, and local laws, ordinances, and regulations which in any manner affect performance under the contract.

**Article 24: Signature Authority, Binding Effect, and Sovereign Immunity**

Service Provider represents and warrants that the individual signing this contract is authorized to sign this document on behalf of Service Provider and to bind Service Provider under this contract. This contract shall be binding upon and shall inure to the benefit of TJJD and Service Provider and to their representatives, successors, and assigns. The parties expressly agree that no provision of this contract is in any way intended to constitute a waiver by TJJD or the State of Texas of any immunities from suit or from liability that TJJD or the State of Texas may have by operation of law.