**ATTACHMENT A**

**SOLICITATION NO. 1310004350**

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

**PURPOSE**

The Contract is awarded on behalf of the Oklahoma Department of Corrections (ODOC) for an advanced cell phone interdiction service/system to detect and locate contraband wireless communication devices to assist in the effective elimination of contraband communications at ODOC locations across the State of Oklahoma.

**BACKGROUND**

As correctional facilities must prevent illicit contraband from being introduced into a controlled environment, ODOC wishes to locate illegal contraband cell phones, smart phones, PDAs, tablets, 2-way pagers, and similar devices. ODOC has twenty-three (23) institutions are they are categorized into four distinct security levels: Maximum Security, Medium Security, Minimum Security and Community Corrections Centers. ODOC wishes to explore and leverage advanced technological options in a pilot program of one or more correctional facilities in order to assess whether this technology improves detection rates of illicit devices beyond that which is already in use.

**1.** **Contract Term and Renewal Options**

The initial Contract term, which begins on the effective date of the Contract, is one year and there are two (2) one-year options to renew the Contract. Renewals to be exercised solely at the discretion of ODOC and will be at the same terms and conditions as the base-year offering. If ODOC wishes to exercise an option year, it will notify the vendor in writing of intention to do so prior to the ending of the existing contract.

**2.** **Scope of Work**

The parties agree to the following terms in addition to obligations set forth in other Contract Documents:

2.1 Supplier must provide entire operating platform (hardware, software, and any other necessary infrastructure necessary to use the System) to accomplish required services, to include adapting to changes as necessary in wireless technologies over the course of the contract as defined in Section 3. Technical Requirements.

2.2 Supplier must ensure all technology offered uses only legally authorized methods and supplier attests that its methodologies do not violate existing state and federal laws. Supplier shall be solely responsible for ensuring compliance with all applicable laws as it relates to the use of their proposed solution.

2.3. Supplier must demonstrate through its bid offering as to why its system will demonstrate detection and location of devices, to include why its offering remains superior to competitors. While prepared sales materials may be submitted in satisfaction of this requirement, suppliers are strongly advised to include any additional narrative as necessary to distinguish its offering from another bidder.

2.4 Supplier will propose and price per system, which is defined as complete turn-key solution meeting all of the requirements of within this attachment. ODOC desires to purchase as many systems as its budget can support and encourages suppliers to offer multi-system discount pricing.

**3. Technical Requirements**

3.1 System must legally detect and locate devices per the following conditions.

3.2 System must demonstrate, or supplier must otherwise provide an appropriate survey of all radio frequencies/channels in use by commercial wireless carriers providing service within the designated pilot program facility(s) in order to determine the detection and geolocation of illicit use of devices.

3.3 Supplier shall be solely responsible for any licensing agreements, including obtaining all required Federal Communications Commission (FCC) licenses or any other approvals needed to utilize its system and shall be solely responsible for ensuring that use of system complies with all federal and state laws and regulations applicable to the use of system.

3.4 System must never interrupt any authorized communication from devices, to include Emergency Calls to 911. System may never disrupt devices outside of correctional perimeter environment, defined as the outer-most perimeter of facility(s) in which system in use. Additionally, system must not interfere with, or otherwise adversely affect any authorized ODOC devices within its facilities, such as Wi-Fi equipment and security radios, or radio and non-cellular communication equipment used by local law enforcement or other authorized users. System must never collect legally protected information in violation of federal and state laws and regulations.

3.5 System must include an audit log which records all operations, detections, and locations as applicable. This log data must be clear, concise, and reasonably understood by users of system without frequent intervention by supplier in order to provide such explanation. Audit log must be capable of self-generating audit report of operations as described within Section 3. Technical Requirements.

3.6 System must provide a remotely adjustable coverage area within a minimum radius of 10 ft. (Ten feet) and detection must occur within milliseconds (virtually simultaneously) from the moment devices begin illicit operations per use of system. Detection must include cellular, Wi-Fi, and Bluetooth Devices as applicable.

3.7 System infrastructure (including all hardware, software, and any other physical infrastructure required in order to use system for its intended purpose and must remain fully compliant with all federal, state, and local building codes, laws, regulations, and industry standards, to include but not limited to:

o National Electric Code (NEC)

o National Fire Protection Association (NFPA)

o Underwriter’s Laboratories (UL)

o National Electrical Manufacturers Association (NEMA)

o Institute of Electrical and Electronic Engineers (IEEE)

o Americans with Disabilities Act (ADA)

o Telecommunications Industries Association (TIA)

o Federal Communications Commission (FCC)

o American National Standards Institute (ANSI)

o Building Industry Consulting Services International standards and best practices. (BICSI)

3.8 System must be appropriate for a maximum security correctional institution. Supplier must follow ODOC security practices including use of only ODOC approved tamperproof security fasteners in all areas inside the institutional perimeter. Supplier must provide written narrative or otherwise provide materials substantiating their ability to effectively deploy system in a correctional environment with reasonable safeguards. Failure to do so may result in bid offering being deemed non-compliant and unacceptable for further consideration. In order to best satisfy this requirement, Supplier is encouraged to provide specific past-performance examples of system use within a correctional environment, as well as business references who may substantiate such use.

3.9 All System collected data shall be considered confidential and any data recorded per use of system shall the property of ODOC and may not be disclosed without ODOC’s written consent of such disclosure

3.10 All system components must be proposed as new, which is defined as without physical blemish or external/internal defects and not otherwise classified as refurbished, reused, recycled, or any other manner where previously used materials have been repaired, refurbished, recycled, to be like new.

3.11. System Design: Supplier must provide a comprehensive implementation plan that includes design, installation, and testing of the proposed system. At a minimum, this must include comprehensive details to complete each of the following:

o System configuration and design.

o Installation and implementation process.

o Testing and demonstration of system readiness prior to active use by ODOC.

o All aspects of design through final system readiness must include a proposed timeline. Timeline defined as reasonable projected number of business days to implement each requirement.

4. **Training/Service/Warranty**

4.1. Supplier must provide initial on-site training per system requirements and industry standards on system operations in each ODOC facility where so employed. Additionally, supplier is encouraged to propose how it will ensure training as applicable to any required system updates or otherwise as refresher training for personnel (either in person or remote). Further, supplier shall be responsible for any required system updates which if not enacted will prevent system from operating as proposed and includes all hardware, software, or other infrastructure as required. System updates defined as required in all instances when failure to implement shall result in reduced or otherwise loss capability of system during the period of contract performance. Any other system updates shall be deemed value-added and ODOC remains under no obligation to accept them. All required updates shall be the sole responsibility of the supplier who will bear all costs of the same.

4.2. Supplier must provide dedicated customer support, which is defined as dedicated customer support to ODOC via phone, email, or other real-time system monitoring technologies. Customer support must include all basic IT help desk capabilities (trouble reporting, tracking status of faults and repairs, etc.). Additionally, supplier must make a reasonably good-faith effort to ensure all on-site repairs are within 10 (ten) business days from date of ODOC reported trouble with system. Should on-site delays result due to supply-chain issues, supplier must provide written notification of such and projected time of arrival for all necessary components to effect repair, as well as projected date by which repairs may be completed.

4.3. Supplier offering must fully describe warranty coverages of system and whether such warranties cover parts, labor, or both. Labor is defined as including any travel required to and from system site. Supplier must fully define and price any service calls which are not included within System warranty coverages.

4.4. Service Credits: Supplier acknowledges ODOC is paying supplier to deliver the system and related services as indicated within Attachment A. If supplier fails to meet the expectations as proposed within supplier offering, then supplier must offer in-kind service credits which reflect the diminished use of system. These credits shall be based on total system cost as proposed, divided by 365 days (to determine daily operational costs) and applied for the number of days in which system either does not function or otherwise substantially fails to meet its system requirements as enumerated within Attachment A. Service credits shall be applied to all system failures which are in no-way connected to user error by ODOC. Additionally, ODOC shall have the right to pursue any legal or equitable remedies as necessary based on the totality of the circumstances.