Attachment A

to

RFP No. 4539

Mississippi Department of Corrections

(MDOC)

Electronic Monitoring Services

ITS Project No. 47571

TABLE OF CONTENTS

I. GENERAL

A. How to Respond to this Section

1. Beginning with Item 17 in Section I. General, label and respond to each outline point as it is labeled in the RFP through Section IV. Implementation and Training Requirements.
2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items in which they disagree.
3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.
4. "WILL COMPLY" indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or Vendor's proposed solution must comply with a specific item or must perform a certain task.
5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V of RFP No. 4539 for additional instructions regarding Vendor exceptions.)
6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B. General Overview and Background

8. The Mississippi Department of Corrections (MDOC) is responsible for overseeing and managing correctional facilities and programs within the state, including electronic monitoring of offenders. Electronic monitoring plays a vital role in enhancing public safety, reducing recidivism, and providing an alternative to incarceration. It allows for the tracking and supervision of participants in the community, ensuring compliance with court-ordered conditions.
9. Recognizing the importance of leveraging technology to support these efforts, MDOC seeks to procure a comprehensive electronic monitoring solution. This includes the acquisition of equipment, central monitoring services, dedicated account management, training, and vendor-provided participant services. The project aims to modernize and streamline the existing electronic monitoring program, incorporating the latest technological advancements and best practices.
10. MDOC currently supervises, on average, 1,500 participants with global positioning satellite (GPS) and zero participants with radio frequency (RF) electronic monitoring. The types of participants supervised electronically include offenders court ordered to the Intensive Supervision Program, offenders assessed by the Parole Board as requiring electronic monitoring as a condition of parole, participants convicted of Failure to Register as a Sex Offender as a condition of Lenora's Law, and some high-risk offenders if designated by the court.
11. The selected Vendor will be tasked with implementing a solution that meets MDOC's specific needs and standards, as outlined in the Scope of Work (SOW). This includes the provision of Radio Frequency (RF) and Global Positioning System

(GPS) monitoring, the establishment of primary and secondary Monitoring Centers, and the provision of locally based staff for participant services.

12. This Request for Proposal (RFP) represents a critical step in MDOC's ongoing commitment to enhancing public safety and participant management. It reflects a collaborative effort between MDOC, ITS, and other stakeholders to identify a Vendor that shares this commitment and has the expertise and innovation to deliver a robust and effective electronic monitoring solution. Through this procurement process, MDOC aims to build a partnership that will contribute to the continued success and evolution of electronic monitoring within Mississippi's correctional system.

C. Procurement Goals and Objectives

13. The procurement process for the Electronic Monitoring Services project is designed to align with the Mississippi Department of Corrections' (MDOC) strategic priorities and operational needs. The primary goal is to identify a qualified Vendor capable of providing innovative, reliable, and cost-effective electronic monitoring solutions. This includes the provision of equipment, central monitoring services, account management, training, and participant services as detailed in the Scope of Work (SOW).

14. Transparency, quality, and collaboration are key objectives throughout the procurement process. We aim to foster an open and competitive environment that encourages participation from a diverse pool of s. Quality and innovation are paramount, and we seek proposals that demonstrate a commitment to best practices, technological advancements, and continuous improvement. Cost-effectiveness without compromising on functionality and compliance with requirements is also a critical consideration.

15. The successful Vendor will be expected to work closely with MDOC and ITS to ensure a seamless transition, implementation, and ongoing management of the electronic monitoring program. Timely delivery, adherence to agreed-upon benchmarks, and a strong focus on public safety standards will be essential for the success of this project. Through this procurement process, we aim to establish a partnership that supports MDOC's mission and enhances the effectiveness and efficiency of electronic monitoring within the state's correctional system.

16. Currently, MDOC contracts with Sentinel to provide a turnkey electronic monitoring solution using global positioning satellite tracking, secure web-based monitoring and data hosting services for approximately 1,500 participants. MDOC has used radio frequency tracking devices for a limited number of participants. Monitoring services provide closed-loop notification (notify with confirmation of Officer call-back verification) and escalating notification (notify, pause for call-back verification, escalate to notify next Officer/contact) twenty-four (24) hours, 7 days a week.

D. Vendor Qualifications

17. The Vendor must have at least three (3) consecutive years of experience delivering Radio Frequency monitoring and/or GPS monitoring services.

18. Vendor must be capable of performing expert On-Site Service and be capable of dispatching expert technicians to the field in the event that problems are encountered requiring diagnosis and potential replacement of hardware components.

19. The proposed monitoring device must have been installed and in use on no less than 1,000 participants through one or more contracts with State, Federal or local government agencies.

20. This experience must include at least six (6) months of active monitoring for the equipment models offered in response to this RFP. The Vendor's experience shall have been met with the Vendor acting as the prime contractor. Identify these agencies, volumes and devices in your proposal response.

21. The proposed base software must have been in use at least six (6) consecutive months in support of one or more contracts with State, Federal or local government agencies.

22. All devices shall be currently registered and approved by the Federal Communications Commissioner (FCC).

23. The equipment manufacturer for the equipment offered in response to this RFP shall have an ISO 9001 certification.

II. FUNCTIONAL/TECHNICAL REQUIREMENTS

A. Radio Frequency Bracelet

24. The bracelet must send encoded radio frequency signals to paired receiver/monitor unit to determine if participant is in prescribed location at MDOC specified times.

25. The strap must be adequate to fit most individuals and must be easily replaced in the field.

26. The covering of the strap of the body worn portion must be made of hypoallergenic material with a high electrical resistance. The strap must have tamper technology to alert in the event of removal or attempt to circumvent monitoring.

27. A tamper alert signal must be sent when an participant enters the range of the receiver/monitor and a tamper occurred while the participant was out of range. If the bracelet is in range when a tamper occurs, notification must be immediate.

28. The bracelet and receiver must be specifically coded to prevent the possibility of two different participants sending the same message for one another via the same receiver. The bracelet must be designed to discourage tracing and duplication of a signal.

29. The bracelet must be easily installed on the participant with minimum training and experience.

30. The Vendor must provide radio-frequency electronic monitoring equipment which must be the most current and updated version of the equipment. In addition, the Vendor must originally have purchased this equipment from the manufacturer.

31. All equipment must be clean in new condition, damage free, and in acceptable operative order. Vendor must identify any and all anticipated products/technologies/services scheduled for discontinuation and/or scheduled end-of-life that are anticipated during the initial term of the Contract.

32. Equipment must be specifically designed as a Radio Frequency (RF) system equipment and must not be derivative components from another tracking system.

33. System must use a body-attached bracelet (Transmitter) and a stationary home-based unit (receiver) to monitor the presence/absence of the Transmitter within a specified range of the receiver and report changes in status and tampering to the

Monitoring Center through standard telephone lines or by cellular telephone service.

34. Transmitters and Receivers must be field replaceable and interchangeable without the need to return them to the Vendor.

35. The Vendor must replace the radio-frequency electronic monitoring system with any future updated and improved version of Vendor's or manufacturer's radio-frequency electronic monitoring system on the request of MDOC and after successful field testing of the updated system at no additional cost.

36. The device must not pose a safety hazard or unduly restrict the activities of the participant. The device must be light weight, small and water-resistant.

37. The Transmitter must be encased in a water-resistant case that is corrosion resistant and impervious to chemical solvents and detergents.

38. The Transmitter must be designed to prevent tracing or duplication of its signal. The Transmitter must have FCC approval for home use. Proposals must include the FCC approval number.

39. The Radio Frequency electronic monitoring system must be capable of providing real-time and batch notification(s) to the Officer on the following violations/alerts:

    a. Non-compliance with pre-determined curfews;
    b. Participant entry and exit at unauthorized times;
    c. Tampering with the Transmitter or any of its components;
    d. Tampering with the Receiver or any of its components;
    e. Failure of the Receiver to report at pre-determined times;
    f. Loss and/or restoration of telecommunications;
    g. Loss and/or restoration of alternating current (AC) power;
    h. Detection of low power or battery malfunctions in the Transmitter or Receiver;
    i. Movement of the Receiver to an unauthorized telephone line;
    j. Detection of operating malfunctions in the Receiver or Transmitter

40. The Vendor must provide either multi-length or sizeable Transmitter straps with replacements provided at no additional cost to MDOC.

41. Neither the Transmitter, receiver, straps, fasteners nor clips, etc. used to install the Transmitter must be available to the general public.

42. The tracking system must provide random location verification of the participant in multiple locations such as home, work, school, and treatment by a telephone or alert device.

43. The tracking systems, at a minimum, should track the participant randomly and on a scheduled basis while at home and away. It should be capable of:

    a. Accurately verifying the presence of the participant/unit.
    b. Confirming the location/phone number of the participant/unit.
    c. Verifying the time of the random/schedule event.
    d. Performing both random and scheduled contacts at predetermined locations and times.

44. The Vendor must provide closed loop alert notification (e.g., receive confirmation from MDOC Agent acknowledging receipt of alert). This level of notification must be

included within each unit's price submitted on the primary proposal price pages (NOT priced as an option.)

B. Electronic Receiver/Monitor

45. The Electronic Receiver/Monitor must receive, send, and monitor radio frequency signals from a paired bracelet. They must confirm presence or absence of an individual at a prescribed location and reports this data to the Monitoring Center.

46. Vendor must provide at least one landline model and one cellular model of Receiver/Monitor Units capable of reporting data. Vendor proposal prices must be inclusive of all communication costs be it landline or cellular.

47. Receiver/Monitor must be reliable to operate in a common home environment.

48. Receiver/Monitor must be easily installed to a standard touch-tone telephone using a standard connector (landline model receiver/monitor only) as well as the standard two-prong AC power source.

49. Receiver/Monitor must be capable of monitoring multiple bracelets simultaneously on one Receiver/Monitor/phone line, each with an independent curfew schedule.

50. Vendor must identify the cellular service providers utilized by the proposed Radio Frequency Cellular unit.

51. Radio Frequency Cellular unit must have technology to detect, ensure, and report that the cellular unit remains in the participant's residence. Vendor must describe the technology used by the proposed device to accomplish this feature.

52. Equipment must be tamper-resistant and have notification capabilities.

53. In the event of power disconnect or commercial outage, the receiver must have a minimum of 48 hours internal, auto-recharging back-up battery to support complete continued functionality, including but not limited to detecting and reporting information.

54. The Receiver must allow use with any brand or make of telephone line including touch tone, broadband, DSL, and VoIP.

55. The Receiver must be able to receive and record any Participant status change, such as when the Participant entered or left the residence, as well as the working condition and tamper status of the Receiver and the Transmitter. The Receiver must have the ability to record the actual time of occurrence.

56. The Receiver must communicate the Participant's status to the Monitoring Center Computer immediately (within one minute) in the event of curfew violations (at expiration of leave window) (including the Transmitter returning within range) or Transmitter tampers.

57. The Receiver must notify the Monitoring Center within one (1) minute of any tamper attempts to the Receiver itself as well as AC power source problems or disconnects. In the event of a telephone line disconnect, the Receiver shall notify the Monitoring Center of stored messages within one (1) minute of restoration of telephone service. All messages must be time and date stamped with actual time of occurrence.

58. At least seven (7) days prior to battery failure, the Transmitter must emit a low battery message to the Receiver and to the Monitoring Center, and must be handled as an alert.

C. Global Positioning Satellite Tracking (GPS)

59. All devices must be shock resistant, waterproof, and function reliably under normal atmospheric and environmental conditions. The device must not pose a safety hazard or unduly restrict the activities of the participant. The GPS device casing must be hardened to withstand the environment it is deployed and be waterproof.

60. The proposed equipment must provide active, passive, and/or hybrid GPS surveillance equipment in conventional unit types. Vendor must provide a description of the monitoring system and capability for each equipment type offered.

61. The device must attach to the participant with either a reusable or a replaceable strap that is adjustable to fit the participant. The strap must only be installed on the participant's ankle. Cost associated with replacement of reusable or disposable straps and frequency of replacement must be included in the cost matrix.

62. The device must be small, lightweight, and not unduly restrict the activities of the participants. Vendor must provide a description and photograph of the GPS device.

63. The device must be supplied with an electronic charger unit that uses a wall outlet power (alternating current) with a charging cord of a minimum of 6 feet long.

64. The device must communicate to the Vendor's Software System by common cellular carrier, with the option of a secondary cellular carrier (list cellular networks proposed).

65. The device must be supplied with an installation kit containing all necessary equipment to install, activate or deactivate the device. At least one tool kit will be included for each 25 units in use.

66. Equipment must be designed so that if an participant tampers with the device an alert is immediately generated.

67. All devices shall be capable of being attached to the participant in a matter that efforts to tamper with or remove the bracelet are obvious upon visual inspection.

68. Vendor's information exchange must be web-based for use by MDOC in enrolling, tracking, and viewing activity/reports/zone management/mapping and accessible via any devices with internet access. This system must be fully web-based and must not require any software to be loaded onto MDOC computers.

69. The device must incorporate non-volatile memory capable of storing at least 24 hours of events (with date and time of occurrence) at times when the cellular service or electrical power may become unavailable. Non-volatile memory must retain unreported events and report them once power/cellular services have been restored, including date and time of occurrence.

70. MDOC prefers a Mobile Application for use by Agents with smart phone devices to enroll participants, deactivate/acknowledge alerts and track participants.

71. Web-based software must allow MDOC to query a location (by address or GPS coordinates) and view all participants within a user-defined radius. This function must be capable in real time as well as available through a query for user defined radius and time frame.

72. Web-based software must allow the MDOC Agent to increase or decrease the level of monitoring (e.g., Passive, Active, etc.) without changing equipment, encountering equipment, contacting the Monitoring Center or alerting the participant that monitoring level is changing.

73. Vendor must allow MDOC to determine reporting intervals and to designate intervals on a per participant basis.

74. The device must also be remotely contacted via the cellular network to force the device to instantly locate and call back with its data immediately (required in all modes – Passive, Active and others). Proposals must include an average of one instant locate per participant per day included in the proposed unit/day pricing at no additional cost.

75. All devices must be capable of utilizing unlimited alternative location tracking using the cellular network in the absence of GPS at no additional cost.

76. The device must have the capability of transmitting reports or violations by phone, text message and email.

77. The device must be capable of producing mapping displays and reports that include participant location, zone violations, tampering & battery status.

78. All levels of GPS (Passive, Active, others) must report violation alerts immediately, including but not limited to those listed below:

    a. Band or Device Tamper
    b. Inclusion Zone Violation
        1. Enter Inclusion Zone by name
        2. Exit Inclusion Zone by name
    c. Exclusion Zone Violation
        1. Enter Exclusion Zone by name
        2. Exit Exclusion Zone by name
    d. Curfew Violation
    e. Failure of device to report to Monitoring Center
    f. Low Battery Indication

79. Device must provide notification of participant violation(s) to MDOC by automated and manual communication. Vendor must provide cost associated with each method of notification.

80. Device must be capable of making schedules active or inactive without deleting them from the participant's record or the system.

81. Web-based software must allow MDOC to organize caseloads by Region, Area and Agent.

82. Web-based software must allow MDOC to include notes related to system-generated alerts. Notes should be capable of being attached to alert within the web-based system.

83. All devices must remain in "tamper alter status" until MDOC has inspected the device and cleared the alert.

84. All devices must have internal, rechargeable, sealed, non-removable battery power.

85. The GPS device must be supplied with a compatible wall charger. The charger must include a charging cord that is at least 6 feet (1.83 meters) in length to ensure adequate accessibility and convenience during charging. The Vendor must specify the type of charger provided (e.g., USB, AC adapter) and confirm that it meets all applicable safety standards.

86. At least seven (7) days prior to battery failure device must provide a signal to indicate that battery power is low, and that the device should be recharged. Vendor must provide a description of their battery and provide information related to the battery life.

87. The Vendor must provide any replacement power sources for use with the GPS Devices that fail under normal use.

88. The Vendor's web-based system and mobile software applications must both provide access to view the current device battery charge and have interactive events to track and report each participant's starting/ending charge time.

89. The Vendor's Monitoring Center Service must provide immediate notification via, text message or email 24 hours a day, seven days a week to designated MDOC staff when an alert notification is generated.

90. The Vendor's web-based system and mobile software applications must include the ability to compare the participant track points to crime locations from law enforcement Record Management Systems. This functionality must have been in use within the past 12 consecutive months, prior to proposal submittal date. The Vendor's experience shall have been met with the Vendor acting as the prime contractor in providing GPS software or equipment. Anytime Beta testing does not count toward the required experience.

91. The Vendor's Monitoring Center service must triage alerts, including triaging and responding to alerts with direct contact to both MDOC staff and participants for resolution as defined by MDOC. The Monitoring Center service must have the ability to escalate an alert notification if the officer does not acknowledge the notification within an MDOC-specified time to the next MDOC designated contact. In the event an alert notification is unresolved, the Vendor's Monitoring Center service shall be responsible for contacting the MDOC's designated officer via, text message, facsimile, email or phone. The means or mode of contact shall be at the MDOC's discretion. These services must be provided twenty-four (24) hours 7 days a week.

92. The battery for the body-attached device must be able to re-charge the battery from a dead battery status to hold a single charge for a minimum period of sixteen (16) hours in two (2) hours or less. The battery for the body worn device must be able to re-charge the battery from a dead battery status to maximum capacity (100% charge) in five (5) hours or less.

93. The body-attached device must have a guaranteed life cycle of not less than twelve (12) months. Each device must be replaced at specific intervals as mutually agreed upon by the Vendor and the Customer to avoid device failures due to loss of battery power.

94. Active GPS must be at a service level that must collect a tracking point at least once every minute and must report information via the cellular network at least once every fifteen (15) minutes and must report tampering and zone violations immediately. Devices proposed for Active GPS that utilize less frequent intervals shall be rejected and not evaluated.

95. Passive GPS must be at a service level that collects a tracking point at least once every one minute and must report information via a cellular or landline telephone at least once every twelve (12) hours.

96. Vendors must offer at least one hybrid service plan that collects a tracking point once every minute and reports information via the cellular network at least once

every 30 minutes. Other hybrid plans may be offered as an “optional” service with separate pricing and description of frequency of tracking points and reporting intervals for each plan proposed.

97. The system must acquire GPS within 5 minutes when placed in an outdoor environment.

98. The GPS device must also have the ability to download location and alert information via landline in areas without adequate cellular coverage.

99. All communications to and from the system’s devices must be encrypted.

100. The Vendor’s system must have the capability to query GPS location information both automatically and individually, including latitude and longitude, and mapping on all participants based on specified distance from a specified location within specified date/time range as means of performing analysis of GPS Participants at a potential crime scene.

101. Any software necessary for MDOC utilization or an interface must be provided at the expense of the Vendor, with no licensing fee to MDOC.

102. The Vendor’s system must enable the user to define a variety of zone types including but not limited to Inclusion, Exclusion, and Mobile Proximity Zones, Zones within a Zone, each with its own governing schedule time/date-based schedule. Describe your web-based capabilities to meet each of these requirements, provide sample screen shots and describe the specific steps involved in configuring a zone with an accompanying schedule.

D. Monitoring Services

103. Vendors must provide 24 hours, 7 days a week staffed monitoring of participants in order to promptly detect unauthorized absences, late arrivals, equipment malfunctions and tampering, and to respond promptly to inquiries from MDOC.

104. All operators answering calls, monitoring, and reporting must be certified by Vendor as to full knowledge of systems and ability to operate systems. All Vendors' monitoring staff must be certified by the Original Equipment Manufacturer and must be well versed in all aspects of the system including but not limited to:

    a. Enrolling participants via the web-based system for immediate activation of all monitoring services;
    b. Activating/installing both monitoring and tracking equipment on participants;
    c. Accessing, reviewing, and changing participant data via the Internet;
    d. Troubleshooting equipment/monitoring/tracking problems;
    e. Terminating participants via the Internet; and
    f. Operators must respond to equipment & system issues, including installation issues.

105. The Vendor must provide toll-free telephone and facsimile numbers for MDOC staff to access the operators, technical support, and customer service specialists at the Monitoring Center.

106. Upon the occurrence of curfew violation, tampering, loss of power, the monitoring system must notify MDOC Agents using the agents’ selected options of notification (e.g., text message, email, telephone call).

107. All curfew and equipment status alerts must be reported to MDOC Staff immediately or upon expired grace period. Alerts shall be reported by web-based system and/or email. Additionally, alert reports may be provided by facsimile and/or telephone on an optional basis. Vendor must have the capability of reporting alerts after applying a defined MDOC grace period for reporting designated events.

108. The Vendor must provide closed loop alert notification (e.g., receive confirmation from MDOC Agent acknowledging receipt of alert). This level of notification must be included within each unit's price submitted on the primary proposal price pages (NOT priced as an option.)

109. The Vendor must describe in detail the ability to provide closed-loop notification (notify with confirmation of Officer call-back verification) and escalating notification (notify, pause for call-back verification, escalate to notify next Officer/contact, pause, continue) and identify any/all system automated capabilities versus manual staff steps required to deliver these types of advanced notification.

110. The Vendor must describe system reporting and/or web-based capabilities to audit the notification steps taken for each alert.

111. The system and software must allow for the following actions over a secure (password-provided by the Vendor) and protected internet or remote access. The Officer shall be able to complete a new participant enrollment including all relevant personal information for each participant, including:

    a. Name, address, telephone number, equipment number, Officer name, curfew information temporary and permanent schedule;
    b. Data/Curfew changes;
    c. Caseload Review, a listing of all active participant names, associated Transmitter/receiver serial numbers, the current real-time status of the participant including the single most recent event that was reported on this participant;
    d. Report Analysis (e.g., Officers shall be able to generate and review monitoring/tracking reports on screen and print hard copies where necessary;
    e. Terminate Participants (e.g., Officers shall be able to terminate monitoring/tracking on any participant on their caseload.)

112. The Vendor's Monitoring Center service must maintain accurate and concise historical logs of all telephone, text message, emails and facsimile calls attempted and completed, including date, time, and the associated incident. The Vendor must make these logs available to MDOC upon request. History must be maintained for six (6) years after termination or expiration of MDOC's contract with the Vendor.

113. The Vendor must maintain a contingency plan for movement of a backup monitoring system/Monitoring Center within 5 hours following a system malfunction.

114. The Vendor must be capable of immediately notifying the designated MDOC Program Manager verbally of any interruption in service or processing delay to the Monitoring Center or telecommunications systems lasting longer than sixty (60) minutes. Such verbal notification shall be provided by the Vendor 24/7/365.

115. The Vendor must provide information on monitoring system architecture to include the hardware, software, and power sources. This must include a description of contingency plans for system failures, such as notifying the MDOC Director of Electronic Monitoring.

116. The Vendor must provide a system of technical support with sufficient experienced personnel to perform remote diagnostics and the ability to troubleshoot equipment problems in a timely manner.

117. The Vendor must have a method for web-based tracking of inquiries for which Vendor will provide a corresponding response (e.g., trouble ticket).

118. Vendor must provide access to designated help desk staff to assist with the needs/concerns of MDOC Agents.

119. Vendors must not employ felons in the performance of this contract. Upon MDOC request, Vendor must provide a copy of employee background check procedures. While it is not necessary for the Vendor to submit these documents with proposal, they must be provided to MDOC post award.

120. The Vendor must maintain redundant inbound and outbound communication services, provided by distinct carriers and/or methods, such that the failure of the primary service or method shall not adversely affect the secondary (backup) service or method.

121. The Vendor must provide MDOC a contact number, accessible twenty-four (24) hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced.

E. Equipment (Spares & Replacements)

122. The Vendor must lease to MDOC all the necessary equipment and provide replacement parts and maintenance of the electronic monitoring system at no additional cost. The Vendor must detail the logistical process to be used to provide and deliver equipment.

123. The Vendor must maintain a stable inventory of equipment at MDOC specified locations. In cases of equipment failure, the Vendor will be responsible for providing replacements and the associated costs.

124. The Vendor must maintain a minimum of twenty percent (20%) spares, based on the number of participants on supervision per county, in good operating condition, and arrange for prompt repair or replacement. The Vendor must be responsible for all replacement and shipping costs. At no additional cost, the Vendor must supply sufficient consumable items (e.g., spare straps and all other necessary parts for attaching and maintaining equipment) to allow timely installation and the servicing of onsite inventory.

125. The Vendor shall provide an Inventory Control Plan / Reports subject to MDOC approval to maintain accurate inventory of both active and spare equipment. While it is not necessary for the Vendor to submit these documents with proposal, they must be provided to MDOC post award.

126. Vendor must include at no additional charge replacements for lost, damaged, stolen equipment up to ten percent (10%) per annum as a percentage of the average number of units in use on participants. Within the price responses, Vendor must provide the per component replacement price for every component of equipment proposed. These prices must be charged only for excess losses, in the event that the included annual ten percent (10%) allowance is exceeded.

127. The Transmitter battery must have a minimum of two (2) year active life and a three (3) year shelf life.

F. Central Monitoring Center

128. Vendor must own and operate both primary and secondary Monitoring Centers that must both be staffed with trained personnel.

129. The secondary (backup) Monitoring Center shall be capable of providing full operational functions in the event the primary Monitoring Center is disabled. The secondary Monitoring Center shall be located sufficiently distant from the primary center, such that it is unlikely to be adversely affected by a manmade or natural event or loss of electrical or communications services that would disable the primary Monitoring Center.

130. The Monitoring Center Facility and Services must have been in use for at least six (6) consecutive months through one or more contracts with State, federal, or multiple-county government agencies at the time of proposal submittal.

131. Monitoring Centers must be located at secured locations with security provisions where access to computer records is restricted to authorized individuals.

132. The Vendor shall maintain a written Disaster Recovery Plan to cover power failures, telephone system failures, local equipment failures, flood or fire at the Monitoring Center and Data Center continued continuity of operations. While it is not necessary for the Vendor to submit these documents with proposal, they must be provided to MDOC post award.

133. The Monitoring Center must have a toll-free telephone service available and accessible 24/7/365 staffed by qualified, technically skilled personnel to troubleshoot monitoring problems.

134. The Monitoring Center must continuously receive and retain all data sent by each receiver/monitor together with the date and time of each occurrence. All telephone calls must be recorded for later playback. All data must be continuously stored electronically, available online in real time and later shall be printable in various report formats.

135. The Vendor must periodically update the system with state-of-the-art computer equipment.

136. The Monitoring Center must have redundant internet and telephone connectivity.

137. The Monitoring Center must provide secure internet connectivity and authentication.

138. Data must be backed up to prevent data loss due to system failure.

139. The Vendor must provide a contingency plan in case of system malfunction that cannot be corrected within four (4) hours.

140. The computer system must be able to retain relevant personal information for each participant. Vendor must provide a copy of the participant profile sheet for review. Vendor must also provide a means to modify this information 24 hours a day.

141. Web-based system must be capable of producing ad hoc and standard reports on demand. Describe and provide examples of standard reports and ad hoc reports provided to other customers.

142. Monitoring Center must have disaster mitigation features (e.g., fire resistant, earthquake resistant; hurricane resistant.)

143. The facility housing the Data Center(s) must have multiple physical security features. Describe the physical security features that protect the Data Center and MDOC data.

144. The Vendor's system must provide for redundancy to avoid unnecessarily excessive downtime due to hardware or software issues. In the event of data disruption, the secondary Data Center must be activated within 60 minutes of initial system failure.

145. The exchange of monitoring information (including enrollment, data changes, monitoring reports and terminations) between Officers and the Vendor's Monitoring Center facility must occur via secure, real-time access to Vendor's web-based system by Officer's using existing MDOC computers/Internet access.

146. The Vendor must ensure that all records (automated or hard copy files) remain the property of MDOC and shall be returned within 30 days, in the event the contract is canceled or terminated.

147. The Vendor must have written policies and procedures for network security, application security, data transmission and data security, as well as Monitoring Center physical security. These documents must be provided if requested by MDOC.

G. Reports and Data Management

148. The Vendor must provide a list of typical detailed reports the Vendor provides to current or previous customers.

149. The Vendor must describe the method of providing the following reports should they be requested by MDOC:

    a. Daily Utilization by MDOC offices
    b. On-demand report containing the serial numbers of each Transmitter and Receiver in use, the participant's name and other MDOC defined data.
    c. On-demand report containing the serial numbers of each Transmitter and Receiver not in In-Service Status
    d. On-demand (user defined date range) report containing the serial numbers of each Transmitter, Receiver and Mobile Receiver (Drive-By) returned to the Vendor from each office during the report week;
    e. On-demand (user defined date range) report containing the serial numbers of each Transmitter, Receiver and Mobile Receiver (Drive By) reported lost, absconded, stolen or not recovered from each region and office during the report week;
    f. On-demand (user defined date range) report containing the serial number of each Drive-By Receiver in the Department's possession during the report month, sorted by Region and office;
    g. Daily active Participant Roster Report.
    h. On-demand reports with user defined fields as requested by MDOC.

150. Upon request from MDOC, the Vendor must provide the most up-to-date complete copy of the System database, including historical data, the data dictionary, file layouts, code tables, code values, data relationships, keys, and indices, etc., in a format requested by MDOC.

151. The Vendor must not release or reveal any data, program information, operation protocols, implementation plans, training material, report(s), publication(s), updates, and/or statistical data related to the Program to any entity, to include non-MDOC personnel, without prior written approval from the MDOC Program Manager.

152. The Vendor must maintain unaltered recorded data of participant violations, to be accessible in original form and substance for utilization as physical evidence for prosecution.

H. Vendor Provided Participant Services

153. The Vendor must provide locally based staff to implement participant-based services. Services may be negotiated based on each user MDOC's needs shall include the following:

a. Participant Enrollment
b. Participant Initial Contact
c. Activate and install devices on participants
d. Monitoring of Participant with Initial Investigation of Alerts with Notification to Officer on Verified Violations
e. Field Service Calls/Maintenance of Equipment
f. Participant orientation
g. Case Management Services
h. Work/school verification
i. Schedule entry/maintenance
j. Collateral office visits to review compliance, adjust schedules.
k. Mobile spot check of Participant

154. The Vendor must describe each service and the associated cost for each service in the cost matrix.

155. The Customer does not guarantee usage of participant services included in the Vendor's proposal.

III. HOSTING ENVIRONMENT

A. General

156. MDOC is seeking a vendor hosted, cloud solution. The cloud hosted environment must be capable of supporting the solution at maximum user as well as maintaining all database functions.

157. Vendor must submit a detailed description of their cloud hosting services. At a minimum, Vendor should address the following:

157.1 Compliance and Certifications: List all relevant compliance/certifications held by Vendor such as SSAE-18, SOC, and FISMA, etc.

157.2 The Vendor must describe their retention scheme for standard server backups.

157.3 The Vendor must describe their plans for databases, applications, auto-run, and on-demand reporting, etc.

157.4 MDOC requires an at-most Recovery Time Objective (RTO) of 24 hours and an at-most Recovery Point Objective (RPO) of 24 hours. Cloud services

must be restored within 24 hours of a service disruption. Production systems must be backed up at least nightly so that the longest possible period of data loss would be 24 hours. Vendor must describe how his services meet or exceed these expectations.

157.5 System uptime must be 99.99%.

B. Business Continuity/Disaster Recovery

158. So that MDOC can assess Vendor's business continuity strengths, Vendor must provide a preliminary business continuity plan that reveals Vendor's ability to analyze, design, implement, test, and maintain cloud services.

159. The business continuity plan must reveal contingency and disaster recovery strategies available to MDOC for the services sought by this RFP. At a minimum, the plan must address such questions and issues as:

159.1 What are the plans, procedures, and technical measures that will restore MDOC services as quickly and effectively as possible following a service disruption? So that MDOC can properly evaluate your response, provide as much detail as possible.

159.2 Is the distance between the backup facility and the primary facility adequate to ensure one incident does not affect both? Do the two sites provide redundant power and networking?

159.3 Describe your process for notifying MDOC when a major event has occurred or is likely to occur that will impact service?

159.4 How do you keep your process and contacts updated?

159.5 Describe the plans for periodically testing business continuity and disaster recovery processes.

160. Upon award, the agreed upon RPO and RTO must be accounted for and documented in the resulting plans for business continuity and disaster recovery.

C. State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy

161. Vendor understands and agrees that all proposed hosting services will comply with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy specified below in this section of this RFP.

162. Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, MDOC must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided below are applicable for State of Mississippi data that MDOC has categorized as public data.

163. Data Ownership: The State of Mississippi (State) shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution, (ii) response to service or technical issues, (iii) as required by the express terms of this service, or (iv) at State 's written request.

164. Data Protection: Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the

Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

a. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.

165. Data Location: The Vendor shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Vendor will permit its personnel and contractors to access State data remotely only as required to provide technical support.

166. Notification of Legal Requests: The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to subpoenas, service of process, or other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

167. Termination and Suspension of Service: In the event of termination of the contract, the Vendor shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of State data.

a. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any State data.

b. Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Vendor shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90-day period, the Vendor shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in section 7(d) below. Within this 90-day timeframe, Vendor will continue to secure and back up State data covered under the contract.

c. Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

d. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.

168. Background Checks: The Vendor shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration of a minimum of one (1) year is an authorized penalty. The

Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.

169. Security Logs and Reports: The Vendor shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an MDOC customer to request reports of activities of a specific user associated with that MDOC. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

170. Contract Audit: The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense.

171. Sub-contractor Disclosure: The Vendor shall identify all its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

172. Sub-contractor Compliance: Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

173. Processes and Procedures: The Vendor shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing — the State and the Vendor shall understand each other's roles and responsibilities.

174. Operational Metrics: The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. Examples include but are not limited to:

    a. Advance notice and change control for major upgrades and system changes
    b. System availability/uptime guarantee/agreed-upon maintenance downtime
    c. Recovery Time Objective/Recovery Point Objective
    d. Security Vulnerability Scanning

175. Encryption: The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

    - The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).
    - The Vendor and the State shall reach agreement on the level of liability

insurance coverage required.

- The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
- At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
- The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.
- The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
- The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.
- The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
- In the event the Vendor fails to always keep in effect the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

176. Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll-free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

IV. IMPLEMENTATION AND TRAINING REQUIREMENTS

A. Account Manager

177. Vendor must provide a dedicated Account Manager to coordinate project management with MDOC's Director of Electronic Monitoring as described in its proposal.

178. Account Manager will serve as the central point of contact to ensure Contract services are provided at a satisfactory level. Such services would include: on-site on-going training to current MDOC and new employees; technical assistance as requested; and resolve issues and ensure customer satisfaction. Customer support may include site visits and assistance with implementation of new phases of electronic monitoring program.

179. Account Manager must provide consulting services and project management support in the transition, implementation, and/or migration of each new equipment model or technology.

180. Vendor and MDOC shall work together to develop implementation plans with specific benchmarks and timelines.

181. Both MDOC and the Vendor shall mutually agree upon implementation plans as well as any subsequent changes.

182. MDOC reserves the right to conduct audits, reviews or any inspection it deems appropriate to ensure that equipment, services and contract commitments are met.

B. Contract Performance Review

183. A monthly report must be provided to the MDOC Director of Electronic Monitoring to track Vendor and system performance during the contract period. The report must provide the following minimum information for the purpose of statewide performance tracking and trending of the program, including but, not limited to the following (Vendor must include a sample of monthly report with the proposal):

    a. Agreed upon key performance indicators for RF
    b. Agreed upon key performance indicators for GPS
    c. Agreed upon key alert statistics for program that can be subdivided into regions and areas.
    d. This report must include agreed upon key performance indicators (e.g., caseloads, inventory, alerts, opened/closed problem ticket items etc.)

184. The Account Manager will ensure that data is accurate and appropriate indicators are tracked.

185. The Account Manager will be responsible for responding to inquiries and ensuring needed corrective actions are taken to ensure consistent performance levels from Vendor as required by the MDOC.

186. Account Manager must work in concert with the MDOC Director of Electronic Monitoring to ensure MDOC has equipment and Vendor support necessary to operate a program that meets MDOC's standards of public safety.

187. Vendor must provide a high-level implementation plan with the proposal response. This plan shall include a timeline for training electronic monitoring agents and support staff and enrollment of participants currently on electronic monitoring. The methodology for importing existing data into a new monitoring system shall be included with the proposal response and with a timeline designated as part of the implementation plan. The final implementation plan will be received within fourteen (14) days of the contract award.

188. The Vendor must make available qualified personnel to provide testimony as requested or subpoenaed. Affidavit, expert witness testimony, violation hearing testimony, or any other GPS expert testimony/certification shall be provided at no additional cost to MDOC. The Vendor must immediately notify MDOC Electronic Monitoring (EM) Program or designee upon receipt of any subpoena involving or affecting MDOC.

C. Training

189. Initial training for MDOC Agents must include on-site formal training with each of the three Regions as part of the implementation plan within 30 days of the start date of MDOC's contract unless an alternate training schedule is agreed upon in writing by the Customer. Ongoing training shall be provided as agreed mutually between Vendor and MDOC.

190. Vendor must travel to each site to assist MDOC staff with installation and enrollment of participants. Vendor must provide all training materials at the Vendor's expense.

191. Annual Meeting - MDOC shall schedule an annual statewide meeting for all Electronic Monitoring Agents. In addition to the Vendor's Account Manager, the Vendor shall have attendance from at least one member of senior executive staff. The purpose of the meeting shall be information-sharing to address pending action items and to provide agents with the opportunity to speak directly to executive management about any concerns they wish to address.

192. Regional Meetings - MDOC shall schedule a regional meeting for all Electronic Monitoring Agents. The Vendor's Account Manager and EM Director shall facilitate the meeting. The purpose of this meeting will be to share information and address pending action items and address electronic monitoring concerns.

193. Webinars or other computer-based training shall be utilized to provide supplemental training after the initial roll-out training, as requested by MDOC within 48 hours of the request.

194. Vendor must provide training and/or user manuals in soft format (such as PDF) and shall authorize MDOC to duplicate these materials as necessary to facilitate MDOC training needs.